

# La Méthode EBIOS désormais adaptée aux traitements de données à caractère personnel et à la CNIL | Denis JACOPINI



La Méthode EBIOS, élaborée par l'ANSSI, initialement prévue pour la gestion des risques informatiques a été adaptée aux traitements de données personnelles. Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

## 1. Objectifs

Dans une entreprise, les risques liés à l'utilisation de l'outils informatique peuvent être classés en deux principales catégories :

- Les risques liés au fonctionnement de l'outil informatique et à la sécurité d'accès au système;
  - les risques liés à l'usage des données présentes dans le système informatique.

La gestion du premier risque est en général déléguée au responsable informatique ou, pour des structures de taille plus importantes, au Directeur ou Responsable des services

d'information (DSI) et, pour des structures de tailles encore plus importantes, confiée au Responsable de la Sécurité des Services d'Information.

Dans la longue liste des recommandations liées à la gestion de ces risques nous trouvons la gestion du fonctionnement du système informatique, la sécurité des données (garantie de pérennité et protection contre la fuite de de données) mais aussi la sécurité du système informatique contre les erreurs de manipulations et actes malveillants.

Par contre, la gestion des risques liés à l'usages des données, et plus particulièrement des données personnelles, est répartie entre l'utilisateur, le responsable des traitements (souvent le chef d'entreprise dans des structures de petite taille) et le correspondant Informatique et libertés.

Si l'utilisateur doit bien veiller à une utilisation responsable en évitant par exemple de quitter son poste sans verrouiller l'ordinateur

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

## 2. Introduction à la méthode EBIOS

Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

La méthode, élaborée et tenue à jour par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en charge notamment, de la protection de l'état, initialement prévue pour être utilisée dans l'analyse de systèmes informatiques complexes, a été simplifiée et adaptée par la CNIL aux traitements de données personnelles et à la protection de la vie privée qui lui est associée

Cet article décrit les étapes de la démarche à appliquer pour réaliser une étude des risques qu'un traitement de Données à Caractère Personnel fait peser sur la vie privée. Il décrit la

manière d'employer la méthode EBIOS dans le contexte spécifique « informatique et libertés ».

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

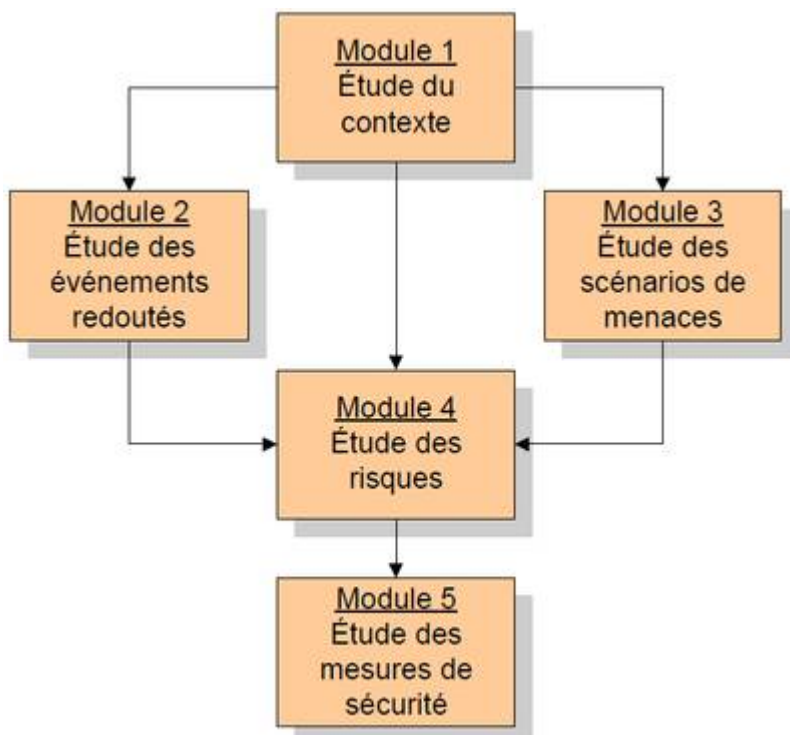
---

### 3. Les 5 étapes essentielles

On souhaite éviter les situations suivantes :

- indisponibilité des processus ;
- modification du traitement (détournement de la finalité, collecte excessive ou déloyale...) ;
- accès illégitime aux Données à Caractère Personnel ;
- modification non désirée des Données à Caractère Personnel ;
- disparition des Données à Caractère Personnel ;

La méthode EBIOS consiste, en fonction de l'environnement de départ, à décomposer en 5 étapes (que nous allons étudier en détail) permettant de passer en revue l'ensemble des mesures préconisées dans leur domaine spécifique, en repérer les points de faiblesses c'est-à-dire les vulnérabilités, d'estimer via une étude de risque, les capacités que semblent avoir les sources de risques à exploiter les vulnérabilités pour réaliser une menace, et enfin de mettre en place des mesures techniques et organisationnelles permettant de remédier aux vulnérabilités qu'elle peut présenter.



1. Etude du contexte :

Quel est le sujet de l'étude ?

Pourquoi et comment va-t-on gérer les risques ?

2. Étude des événements redoutés :

Quels sont les événements craints ?

Quels seraient les plus graves ?

3. Étude des menaces :

Quels sont les scénarios possibles ?

Quels sont les plus vraisemblables ?

4. Étude des risques :

Quelle est la cartographie des risques ?

Comment choisit-on de les traiter ?

5. Étude des mesures de sécurité :

Quelles mesures devrait-on appliquer ?

Les risques résiduels sont-ils acceptables ?

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

## 4. Les 5 étapes en détail

### 4.1. Etude du contexte : De quoi parle t-on ?

Le but de cette étape est d'obtenir une vision claire du périmètre considéré en identifiant tous les éléments utiles à la gestion des risques, en répondant aux questions suivantes :

#### 4.1.1 Quels sont les éléments à protéger ?

- Quel est le traitement concerné ?
- Quelle est sa finalité (voir les articles 6 et 9 de la loi Informatique et Libertés )?
- Quels sont ses destinataires ?
- Quel est le processus métier que le traitement permet de réaliser ?

- Quelles sont les personnes concernées par le traitement ?
- Comment les processus légaux vont-ils être mis en oeuvre ?
- Quelles sont les DCP du traitement considéré ?
- Quelles sont les DCP utilisées par les processus légaux ?

#### 4.1.2 Quels sont les supports des éléments à protéger ?

- Quels sont les matériels (ordinateurs, routeurs, supports électroniques...) ?
- Quels sont les logiciels (systèmes d'exploitation, messagerie, base de données, applications métier...) ?
- Quels sont les canaux informatiques (câbles, WiFi, fibre optique...) ?
- Quelles sont les personnes impliquées?
- Quels sont les supports papier (impressions, photocopies...) ?
- Quels sont les canaux de transmission papier (envoi postal, circuit de validation...) ?

#### 4.1.3 Quels sont les principaux bénéfices du traitement pour les personnes concernées ou la société en général ?

#### 4.1.4 Quelles sont les principales références à respecter (réglementaires, sectorielles...) ?

#### 4.1.5 Quelles sont les sources de risques pertinentes qui peuvent être à l'origine de risques dans le contexte particulier du traitement considéré ?



- Quelles sont les personnes internes à considérer (utilisateur, administrateur, développeur, décideur...) ?
- Quelles sont les personnes externes à considérer (client, destinataire, prestataire, concurrent, militant, curieux, individu malveillant, organisation gouvernementale, activité humaine environnante...) ?
- Quelles sont les sources non humaines à considérer (sinistre, code malveillant d'origine inconnue, phénomène naturel, catastrophe naturelle ou sanitaire...) ?

## 4.2 Étude des événements redoutés : Que craint-on qu'il arrive ?

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de tous les événements redoutés dans le cadre du traitement considéré et d'en mesurer leur valeur de danger.

Pour expliciter les événements redoutés, leurs impacts potentiels doivent être identifiés :

quelles pourraient être les conséquences sur l'identité des personnes concernées, leur vie privée, les droits de l'homme ou les libertés publiques pour chacun des événements redoutés, c'est-à-dire si :

- les processus légaux n'étaient pas disponibles ?
- le traitement était modifié ?
- une personne non autorisée accédait aux DCP ?
- les DCP étaient modifiées ?
- les DCP disparaissaient ?

Afin de hiérarchiser les événements redoutés, la gravité est déterminée en mesurant la facilité avec laquelle on peut identifier les personnes concernées et l'importance des dommages des impacts potentiels.

**Avec quelle facilité peut-on identifier les personnes concernées ? (1 à 4)**

- 1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des Données à Caractère Personnel les concernant (ex. : prénom seul à l'échelle de la population française).
- 2. Limité : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).
- 3. Important : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).
- 4. Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à l'échelle de la population française).

**Quelle serait l'importance des dommages correspondant à l'ensemble des impacts potentiels ? (1 à 4)**

- 1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).
- 2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...).

- 3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...).
- 4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès...).

**Mesure de la gravité = Facilité d'identification des personnes + importance des dommages**

Caractère identifiant + caractère préjudiciable	Gravité correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

#### 4.3 Étude des menaces : Comment cela peut-il arriver ?

Cette étape est optionnelle si la gravité précédemment calculée est négligeable (1) ou limitée (2).

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de toutes les menaces qui permettraient aux événements redoutés de survenir.

## Vulnérabilités des supports

Risque à anticiper :

- Détérioration d'un matériel (ex. : destruction d'un serveur)
- Usage anormal d'un logiciel (ex. : maladresse en manipulant les fichiers)
- Départ d'une personne (ex. : démission de celui qui connaît les procédures)
- Disparition d'un canal papier (ex. : changement de procédures)
- Vol d'un matériel (ex. : vol d'un PC portable dans le train)
- Détournement d'usage d'un logiciel (ex. : usage à titre personnel)
- Modification d'un logiciel (ex. : propagation d'un virus)

Dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ?

- 1. Négligeable : il ne semble pas possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
- 2. Limité : il semble difficile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
- 3. Important : il semble possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).

- 4. Maximal : il semble extrêmement facile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

## **Capacités des sources de risques sont estimées pour chaque menace**

Quelles sont leurs capacités à exploiter les vulnérabilités (compétences, temps disponible, ressources financières, proximité du système, motivation, sentiment d'impunité...) ?

- 1. Négligeable : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints).
- 2. Limité : les sources de risques ont quelques capacités, mais jugées peu importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges restreints).
- 3. Important : les sources de risques ont des capacités réelles, jugées importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges d'administration illimités).
- 4. Maximal : les sources de risques ont des capacités certaines, jugées illimitées, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges d'administration illimités).

**Vraisemblance des menaces = Mesure de la vulnérabilités des supports + Capacités des sources de risques**

Vulnérabilités des supports + capacités des sources de risques	Vraisemblance correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

## Exemples de menaces qui peuvent affecter la confidentialité

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
C01. Usage anormal d'un matériel	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles...	Utilisable en dehors de l'usage prévu...
C02. Espionnage d'un matériel	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance...	Permet d'observer des données interprétables, émet des signaux compromettants...
C03. Modification d'un matériel	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
C04. Perte d'un matériel	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique...	Petite taille, attractif (valeur marchande)...
C05. Détournement d'usage d'un logiciel	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de <i>spams</i> depuis la messagerie, détournement de fonctions réseaux...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
C06. Analyse d'un logiciel	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes...	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source...
C07. Modification d'un logiciel	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
C08. Écoute passive d'un canal informatique	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi...	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables...
C09. Espionnage d'une personne à distance	Divulgaration involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle...	Peu discret (loquace, sans réserve...), routinier (habitudes facilitant l'espionnage récurrent)...
C10. Manipulation d'une personne	Influence (hameçonnage, filoutage, ingénierie sociale, corruption...), pression (chantage, harcèlement moral...)...	Influenable (naïf, crédule, obtus, faible estime de soi, faible loyauté...), manipulable (vulnérable aux pressions sur soi ou son entourage)...
C11. Récupération d'une personne	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation...	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel...
C12. Visualisation d'un document papier	Lecture, photocopie, photographie...	Permet d'observer des données interprétables...
C13. Vol d'un document papier	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut...	Portable...
C14. Espionnage d'un canal papier	Lecture de parapheurs en circulation, reproduction de documents en transit...	Observable...

## Exemples de menaces qui peuvent affecter l'intégrité

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
I01. Modification d'un matériel	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
I02. Usage anormal d'un logiciel	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
I03. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
I04. Attaque du milieu via un canal informatique	<i>Man in the middle</i> pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)...	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération...), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds...)...
I05. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences...	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement...
I06. Manipulation d'une personne	Influence (rumeur, désinformation...)...	Influençable (naïf, crédule, obtus...)...
I07. Falsification d'un document papier	Modification de chiffres dans un dossier, remplacement d'un document par un faux...	Falsifiable (support papier au contenu modifiable)...
I08. Manipulation d'un canal papier	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires...	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier ...

## Exemples de menaces qui peuvent affecter la disponibilité









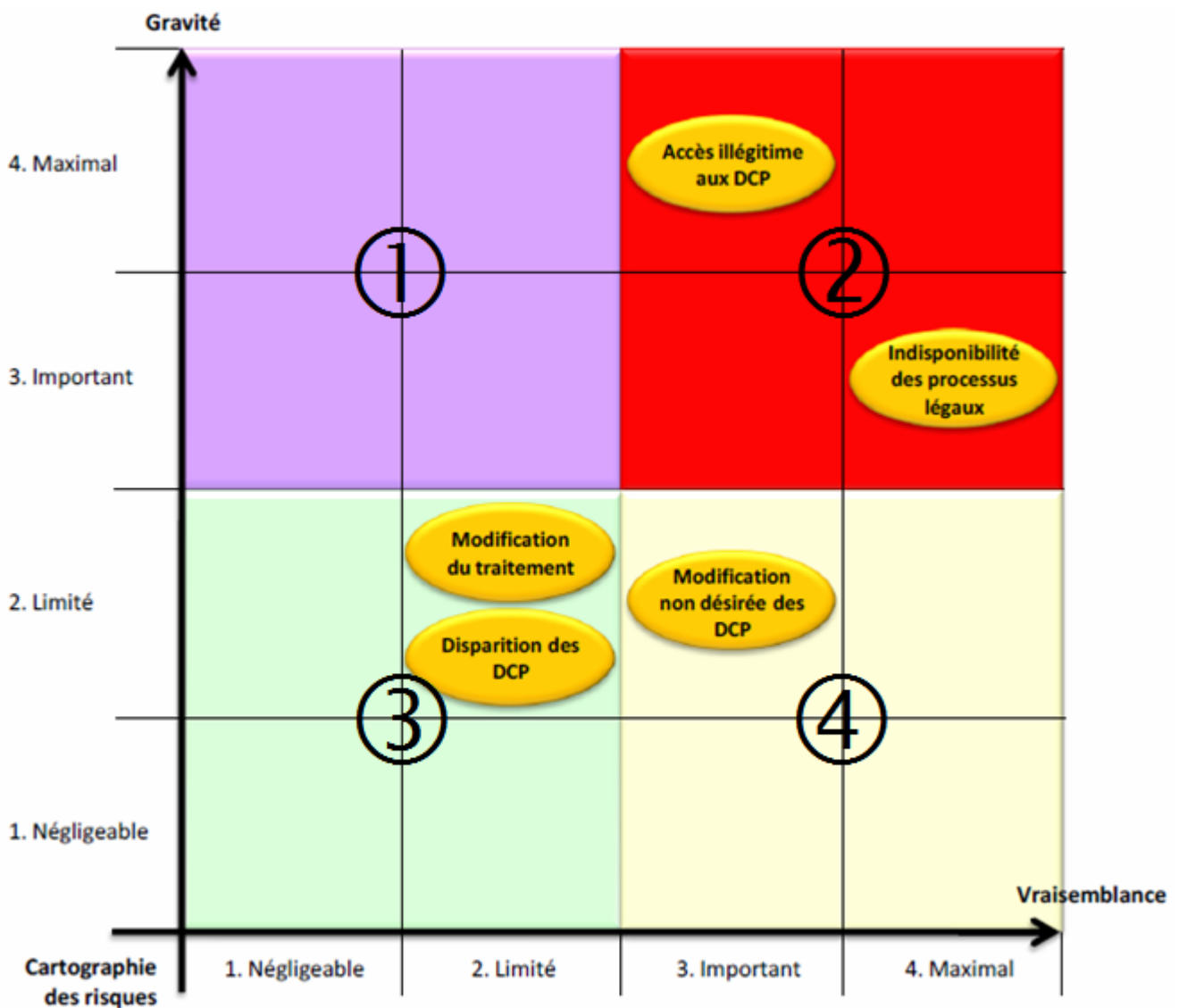
Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
D01. Détournement d'usage d'un matériel	Stockage de fichiers personnels, utilisation à des fins personnelles...	Utilisable en dehors de l'usage prévu...
D02. Dépassement des limites de fonctionnement d'un matériel	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive...	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension...
D03. Modification d'un matériel	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
D04. Détérioration d'un matériel	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage...	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement...) n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires...)...
D05. Perte d'un matériel	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel...	Portable, attractif (valeur marchande)...
D06. Usage anormal d'un logiciel	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
D07. Dépassement des limites d'un logiciel	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues...	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable...
D08. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
D09. Suppression de tout ou partie d'un logiciel	Effacement d'un exécutable en production ou de code sources, bombe logique...	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications...)...
D10. Perte d'un logiciel	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données...	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne...), attractif (rare, novateur, grande valeur commerciale...), cessible (clause de cessibilité totale dans la licence...)...
D11. Saturation d'un canal informatique	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet...	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée...)...
D12. Dégradation d'un canal informatique	Sectionnement de câblage, mauvaise réception du réseau wifi...	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné...), unique...
D13. Disparition d'un canal informatique	Vol de câbles de transmission en cuivre...	Attractif (valeur marchande des câbles...), transportable (léger, dissimulable...), peu visible (oubliable, insignifiant, peu remarquable...)...
D14. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences...	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement...
D15. Atteinte d'une personne	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique...	Limites physiques, psychologiques ou mentales...
D16. Départ d'une personne	Changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation...	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel...
D17. Effacement d'un document papier	Effacement progressif avec le temps, effacement volontaire de parties d'un texte...	Modifiable (support papier au contenu effaçable).
D18. Dégradation d'un document papier	Vieillesse de documents archivés, embrasement des dossiers lors d'un incendie...	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement...), n'est pas approprié aux conditions d'utilisation...
D19. Disparition d'un document papier	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut...	Portable...
D20. Saturation d'un canal papier	Surcharge de courriers, surcharge d'un processus de validation...	Existence de limites quantitatives ou qualitatives..
D21. Dégradation d'un canal papier	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève...	Instable, unique...
D22. Modification d'un canal papier	Modification dans l'expédition des courriers Réorganisation de circuits papier, changement de langue professionnelle...	Modifiable (remplaçable...)...
D23. Disparition d'un canal papier	Réorganisation supprimant un processus, disparition d'un transporteur de documents...	Utilité non reconnue...

#### 4.4 Étude des risques : quel est le niveau des risques ?

Le but de cette étape est d'obtenir une cartographie des risques permettant de décider de la priorité de traitement. Puisqu'un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne :

- sa gravité est égale à celle de l'événement redouté,
- sa vraisemblance est égale à la valeur la plus élevée de la vraisemblance des menaces associées à l'événement redouté.

On peut dès lors positionner les risques sur une cartographie :



En fonction du positionnement de vos risques au sein de la cartographie ci-dessus, vous pouvez par ordre de priorité, vous fixer des objectifs :

Zone n°1 : La gravité des risques est élevée, mais la vraisemblance faible

Ces risques doivent être évités ou réduits, par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devront être privilégiées ;

Zone n°2 : La gravité et la vraisemblance sont élevées

Ces risques doivent absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;

Zone n°3 : La gravité et la vraisemblance sont faibles

Ces risques peuvent être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Zone n°4 : La gravité est faible mais la vraisemblance élevée

Ces risques doivent être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devront être privilégiées ;

#### **4.5 Étude des mesures de sécurité : Quelles mesures devrait-on appliquer ?**

Le but de cette étape est de bâtir un dispositif de protection qui permette de traiter les risques de manière proportionnée, qui soit conforme à la Loi informatique et Libertés, et qui tienne compte des contraintes du responsable de traitement

(légales, financières, techniques...).

Tout d'abord, il convient de déterminer les mesures pour traiter les risques. Pour ce faire, il est nécessaire de relier les mesures existantes ou prévues (identifiées précédemment dans l'étude ou dans les références applicables) au(x) risque(s) qu'elles contribuent à traiter.

Des mesures sont ensuite ajoutées tant que le niveau des risques n'est pas jugé acceptable.

Cette action consiste à déterminer des mesures complémentaires qui vont porter :

1. sur les éléments à protéger : mesures destinées à empêcher que leur sécurité ne puisse être atteinte, à détecter leur atteinte ou à recouvrer la sécurité informer les personnes concernées, minimiser les DCP, anonymiser les DCP...) ;
2. puis, si ce n'est pas suffisant, sur les impacts potentiels : mesures destinées à empêcher que les conséquences du risque ne puissent se déclarer, à identifier et limiter leurs effets ou à les résorber (sauvegarder, contrôler l'intégrité, gérer les violations de DCP...) ;
3. ensuite, si ce n'est pas suffisant, sur les sources de risques : mesures destinées à les empêcher d'agir ou de concrétiser le risque, à identifier et limiter leur action ou à se retourner contre elles (contrôler les accès physiques et logiques, tracer l'activité, gérer les tiers, lutter contre les codes malveillants...)  
;
4. enfin, si ce n'est pas suffisant, sur les supports : mesures destinées à empêcher que les vulnérabilités puissent être exploitées, à détecter et limiter les menaces qui surviennent tout de même ou à retourner à

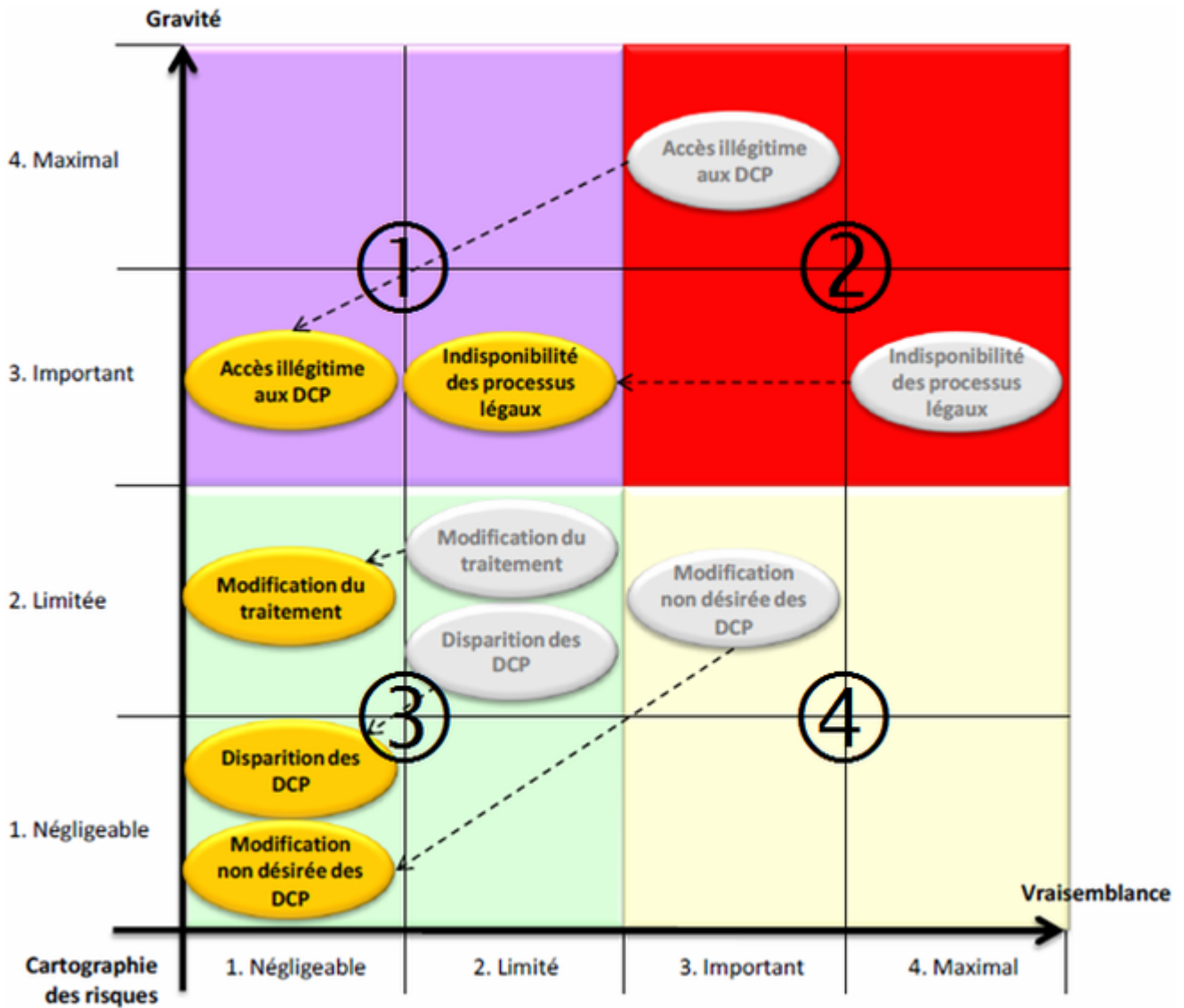
l'état de fonctionnement normal (réduire les vulnérabilités des logiciels, des matériels, des personnes, des documents papiers...).

**Remarque :**

Plus les capacités des sources de risques sont importantes, plus les mesures doivent être robustes pour y résister.

Par ailleurs, les éventuels incidents qui auraient déjà eu lieu, notamment les violations de DCP, ainsi que les difficultés rencontrées pour mettre en oeuvre certaines mesures, peuvent servir à améliorer le dispositif de sécurité. Les mesures spécifiées devraient être formalisées, mises en place, auditées de manière régulière et améliorées de manière continue.

Il convient ensuite de ré-estimer la gravité et la vraisemblance des risques résiduels (c'est-à dire les risques qui subsistent après application des mesures choisies) en tenant compte de ces mesures complémentaires. Il est alors possible de les repositionner sur la cartographie ci-dessous :



Enfin, il convient d'expliquer pourquoi les risques résiduels peuvent être acceptés.

Cette justification peut s'appuyer sur les nouveaux niveaux de gravité et de vraisemblance et sur les bénéfices du traitement identifiés précédemment (prise de risques au regard des bénéfices attendus) en appliquant les règles suivantes :

Zone n°1 : Risques dont la gravité est élevée mais la vraisemblance faible

Ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et



si leur vraisemblance est négligeable ;

Zone n°2 : Risques dont la gravité et la vraisemblance sont élevées

Ces risques ne doivent pas être pris ;

Zone n°3 : Risques dont la gravité et la vraisemblance sont faibles

Ces risques peuvent être pris.

Zone n°4 : Risques dont la gravité est faible mais la vraisemblance élevée : ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;

**Remarque :**

Il peut être acceptable de déroger à ces règles, mais uniquement s'il est démontré que les bénéfices du traitement sont largement supérieurs aux risques.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

## Références :

[http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/CNIL-Guide\\_Securite\\_avance\\_Methode.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf)

<http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html>

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous à plu ? Laissez-nous un commentaire  
(notre source d'encouragements et de progrès)

---

# Les petites entreprises aussi victimes de cybercriminalité | Denis JACOPINI

x	Les petites entreprises aussi victimes de cybercriminalité
---	---

**Vol de données clients, piratage de propriété intellectuelle... les cyberattaques sont légion, mais les petites entreprises se croient souvent peu concernées. A tort. Pour se protéger de ces actes malveillants, une bonne « hygiène numérique » simple à mettre en place s'avère nécessaire.**

« Dirigeant d'une petite entreprise, vous pensez n'avoir jamais été victime d'une cyberattaque ? Soit vous ne l'avez pas détectée, soit vous n'intéressez plus personne et il faudrait penser à changer de métier ! » .

Cette boutade, destinée à faire prendre conscience aux patrons de PME des risques qu'ils encourent face aux hackers en tout genre, émane du contre-amiral Dominique Riban, directeur général adjoint de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information.

Il faut dire que pour une PME, détecter ne serait-ce que les incidents de sécurité, autrement dit le fait qu'un pirate essaie de s'introduire dans le système sans y parvenir, s'avère bien compliqué. Idem pour les attaques. Certes, des comportements bizarres de l'ordinateur peuvent attirer l'attention, comme son ralentissement, des connexions qui s'effectuent toutes seules, la flèche de la souris qui se ballade... Mais les « méchants » savent surtout se faire discrets. Et il s'agit d'un sujet très – trop – technique, lorsqu'on ne possède pas un collaborateur spécialisé à plein temps pour s'en préoccuper...

#### Peu de PME portent plainte

Difficile d'avoir des chiffres fiables sur la réalité de la cybercriminalité subie par les PME. Pour une raison simple: peu portent plainte, lorsqu'elles en sont victimes. Pourquoi risquer la mauvaise publicité ? Retrouver l'auteur de l'infraction s'avère de toute façon souvent mission impossible, admet Jean-Louis Di Giovanni, associé PwC du département Litiges et Investigations auteur d'une enquête sur les fraudeurs en entreprises\* : « On peut remonter sa trace, mais quand l'adresse IP provient d'un cybercafé aux alentours de la gare de l'Est, comment voulez-vous mettre la main dessus ? ». Devenir cybercriminel est en tout cas à la portée de tous. « Aujourd'hui, pour une centaine d'euros, vous disposez d'une solution pour attaquer le système d'information de votre concurrent, ou, pour trois fois moins cher, son smartphone », indique Dominique Riban.

#### Une menace à plusieurs visages

Fomentée par de malveillants collaborateurs, actuels ou anciens, ou bien perpétrée par des hackers externes, la cybercriminalité s'avère multi-formes. Les attaques ciblées, qui visent à voler un savoir-faire particulier ou des données sensibles (secrets de fabrication, brevets, plans industriels, fichiers clients...), côtoient des attaques que Philippe Humeau, directeur général de NBS System, spécialisée dans l'hébergement de haute sécurité et les tests d'intrusion, nomme d'« opportunistes » : « Il suffit que l'entreprise ait un bout de son système connecté sur le net, qu'elle laisse traîner un mot de passe par défaut, et ça y est, elle est vulnérable. Il faut savoir qu'une adresse IP est scannée vingt fois par jour, explique-t-il. Une vraie industrie, que ces scanners qui recherchent des données relatives à des cartes bleues ou à des « identités », autrement dit à des informations sur les personnes (celles que l'entreprise doit signaler détenir à la Cnil, ndr). Aux commandes, des pirates qui effectuent de la récupération massive de données de ce type, puis les revendent au détail à d'autres pirates. » Car elles ont de la valeur. Des données bancaires se revendent dix dollars. Une « identité », entre 5 et 15 dollars. « Une filière aussi organisée que le recel de bijoux », confirme Dominique Riban.

#### Des piégeurs pros

Parfois, les cybercriminels entrent carrément en contact avec l'entreprise. Leur inventivité sans faille leur permet de s'engouffrer dans toute nouvelle brèche. Dernier coup à la mode, la « fraude Sepa ». Les entreprises ont, rappelons-le, jusqu'au 31 juillet 2014 maximum, pour opérer leur migration afin d'être conforme à ces nouvelles normes de paiement européennes. Une aubaine, pour les fraudeurs.

Jean-Louis Di Giovanni détaille le processus : « Quelques jours auparavant, ils envoient un mail à la société, pour l'avertir qu'ils vont la contacter par téléphone afin de procéder à des essais. Le mail semble officiel évidemment. On y trouve le numéro du fraudeur, et, comble du raffinement, si l'on appelle, on tombera sur la petite musique d'attente officielle de la banque. Le jour J, ils téléphonent donc à l'entreprise, et demandent à leur interlocuteur de télécharger un programme... qui sert en réalité à prendre la main sur son ordinateur. Le fraudeur voit sur l'écran toutes les informations qu'aurait normalement la banque, et cela le rend ainsi crédible pour passer un ordre, du type : allez sur le compte x sur lequel vous disposez de 2,5 millions d'euros et faites un virement vers ce numéro de compte étranger. » Nombreuses ont été les entreprises à s'exécuter. 48 h plus tard – le délai maximum pour faire bloquer in extremis le virement – c'est trop tard !

#### 80 % de risques évités avec des mesures simples

Des mesures de protection sont aujourd'hui nécessaires. Contrairement aux idées reçues, le recours à des solutions « technologiques » ne constituerait pas forcément la meilleure arme de défense contre les hackers. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PwC, spécialiste de la cybersécurité.

L'Anssi publie sur son site un mode d'emploi pour éviter les incidents. Il s'agit d'une quarantaine de « règles d'hygiène », concernant la sécurité des messageries, du poste de travail, des imprimantes etc. Une quinzaine sont applicables par les petites entreprises. « 80 % des attaques n'auraient pas lieu si ces recommandations étaient respectées », assure Dominique Riban. Parmi elles, des gestes simples... mais trop souvent négligés. Une évidence, par exemple, de toujours utiliser des mots de passe solides? « 70 % d'entre eux sont faibles, se désole Philippe Humeau. Cette négligence généralisée cause énormément de désastres. Sans compter que les gens utilisent les mêmes partout. »

En plus du choix de mot de passe costauds, les experts font trois recommandations essentielles :

#### 1. Des mises à jour régulières

Se doter d'au moins deux anti-virus et les remettre à jour. « Même si un antivirus n'a jamais été la panacée », concède le contre-amiral Riban. Même nécessité de remise à jour pour tous ses logiciels. « Si les éditeurs font évoluer leurs versions, c'est parce qu'ils ont constaté des failles de sécurité, pointe Philippe Humeau. Mieux vaut éviter de reporter sans cesse le « rebootage » de sa machine quand elle le demande. »

#### 2. Attention au cloud

Toute nouvelle pratique engendre de nouvelles menaces. C'est le cas du cloud. « N'y stockez pas de données cruciales, exhorte Dominique Riban. Privilégiez des opérateurs français dont vous trouverez la liste sur le site de l'Anssi. Je ne dis pas qu'il n'y aura pas d'accident, mais au moins, notre structure a analysé leur façon de travailler, les a audités, leur a fait corriger leurs failles. Ce n'est pas le cas, par exemple, avec Google ou Microsoft. »

#### 3. Haro sur le BYOD

Philippe Humeau n'hésite pas également à pointer du doigt ce qu'il appelle le « problème des jeunes générations » : « Elles débarquent dans l'entreprise avec des notions de sécurité et de vie privée assez light. Elles ont encore moins de réflexes que leurs aînées. Lorsqu'un jeune n'hésite pas à dévoiler sa cuitte du week-end sur Facebook, il ne faut pas s'attendre à ce qu'il sache mettre des barrières là où il devrait les mettre. » Souvent associé à la génération Y – mais pas que –, le phénomène BYOD (« bring your own device ») tient du fléau en matière de cybersécurité. La pratique nécessite d'être encadrée.

« Il devient difficile de l'interdire, mieux vaut donc accompagner l'usage », préconise Philippe Humeau. Mettre en place par exemple un réseau internet privé et un autre public, pour que les collaborateurs s'y connectent avec leur machine. Dominique Riban se montre, lui, beaucoup plus radical : « Même si l'appareil appartient à l'employé, seul l'employeur doit pouvoir administrer la machine, afin que l'utilisateur, ou ses enfants, ne puisse pas télécharger tout et n'importe quoi le week-end ou désactiver l'anti-virus. » Pas sûr que les collaborateurs acceptent...

#### Procéder ou pas à un test d'intrusion

Pour évaluer la capacité de résistance de son système informatique, on peut évidemment faire effectuer un test d'intrusion. A une petite entreprise, il en coûtera aux alentours de 7000 euros. Une facture qui peut paraître prohibitive. « Evidemment cela ne s'adresse pas à tout petit entrepreneur », se défend Philippe Humeau, dont la société propose de tels tests. Mais si l'on a des secrets de fabrication, la dépense est justifiée. Nos interventions se déroulent encore malheureusement trop souvent en post-mortem, nous faisons peu de prévention. »

\* Selon cette récente étude, la cybercriminalité est la 2ème fraude la plus signalée en France. Son évolution inquiète particulièrement les dirigeants qui la classent comme la fraude la plus redoutée dans les 24 mois à venir.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : [http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri\\_1518760.html](http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri_1518760.html)

---

# Comment gérer les licences des logiciels installés par les salariés ? | Denis JACOPINI



Dès que l'on souhaite accueillir les terminaux personnels des collaborateurs dans l'entreprise, il faut absolument se pencher sur la question des licences logicielles pour éviter de cuisantes déconvenues.

Dès qu'un logiciel est présent, les risques liés aux licences sont forcément tapis dans l'ombre. Si l'on souhaite accueillir les terminaux personnels des collaborateurs avec un projet BYOD (Bring Your Own Device), il faut donc se pencher sur la question pour éviter de cuisantes déconvenues. Il en va de même avec les petits logiciels gratuits que les employés peuvent installer sur les équipements fournis par l'entreprise, qu'ils en soient ou non administrateurs.

Ces deux exemples, aussi concrets que courants, offrent quelques clefs pour mieux maîtriser un phénomène dont la complexité et l'ampleur ne cessent de croître.

## **Bring your own licence illégale**

Si l'on ne parvient pas à endiguer un phénomène, autant en tirer profit. C'est notamment le cas avec ces équipements informatiques personnels que les employés introduisent discrètement dans les systèmes d'information d'entreprise depuis des années. Las de lutter, les DSI cèdent à une nouvelle mode : le BYOD (Bring Your Own Device).

Certains se contentent de canaliser ces terminaux hétéroclites en veillant à la survie des équipes de support et à la sécurité de l'information : pas de support technique, connexion sur les accès Wi-Fi pour visiteur, etc. D'autres vont plus loin, comme dans cette grande organisation du secteur tertiaire dont je tairai le nom :

- Les collaborateurs peuvent utiliser leur matériel préféré à la place de celui fourni par la DSI ;
- Ils doivent alors y installer l'antivirus homologué dont une licence leur est allouée ;
- S'ils restituent le PC de la compagnie pour n'utiliser que le leur, ce dernier est subventionné ;
- En pareil cas, ils sont livrés à eux-mêmes en termes d'assistance et de logiciels ;
- Ils peuvent cependant bénéficier de l'accord passé avec Microsoft pour acquérir une licence Office à 13 €.

Remarquable exemple de modernité et d'ouverture, qui permet au passage de réduire les coûts de matériel, de logiciel et de support. Le tout est savamment enrobé d'une communication du plus bel effet vantant les mérites d'une transformation digitale soucieuse des collaborateurs et de leur bien-être.

Comme d'habitude, le diable est dans les détails, en l'occurrence dans les conditions d'utilisation de la licence Microsoft Office à 13 €. En effet, elle couvre l'usage secondaire du logiciel sur un PC personnel si une licence entreprise est octroyée à l'utilisateur. Dans notre cas, l'utilisateur n'a plus de licence entreprise puisqu'il l'a restituée en même temps que son PC.

Voilà comment une organisation peut pousser ses collaborateurs à agir illégalement, sans s'exposer directement puisque les logiciels et les terminaux incriminés ne lui appartiennent pas. Les employés mis en défaut par Microsoft pourront cependant prouver qu'ils ont respecté les préconisations relayées par leur hiérarchie. Il n'est pas certain que cela engendre l'atmosphère voulue : décontractée et propice au travail.

## **La gratuité peut coûter cher**

Une autre situation classique, en apparence anodine, peut faire des remous si l'on n'y prend pas garde : les logiciels gratuits, si pratiques et si sympathiques.

Ainsi, un collègue m'a récemment présenté les bienfaits d'un petit freeware qui le comblait d'aise. Il m'a vivement conseillé de l'installer sur mon PC professionnel. Je l'ai donc téléchargé depuis le site de l'éditeur. Avant de lancer l'installation, j'ai lu les conditions d'utilisation (vous auriez évidemment fait la même chose à ma place). Au milieu de cette prose, j'ai découvert que le produit ne devait pas être utilisé en entreprise. Que l'on travaille sur un terminal personnel ou mis à disposition par la DSI ne change rien puisqu'il s'agit toujours d'un usage « en entreprise ». Utiliser ainsi la version gratuite du logiciel est donc illégal.

Disposer des droits d'administrateur sur son ordinateur n'est pas forcément nécessaire pour installer un tel produit. L'entreprise peut donc se retrouver dans une posture inavouable, même si elle a correctement sécurisé son parc informatique. Pour mettre un peu de piment, ajoutons que ces installations occultes passent inaperçues lors des inventaires logiciels, puisqu'ils sont le plus souvent conçus pour détecter ce qui est connu, et non pour découvrir l'inconnu.

De nos jours, les logiciels communiquent presque tous avec leur éditeur via Internet au moyen de protocoles réseau qui franchissent allègrement les dispositifs de sécurité. Il peut s'agir de rechercher des mises à jour ou de fournir des données vous concernant. C'est légal puisque spécifié dans le contrat de licence accepté *de facto* lors de l'installation, qu'il ait été lu ou non. Il suffit alors d'un nombre significatif de PC communiquant depuis votre réseau d'entreprise pour mettre la puce à l'oreille de l'éditeur. Il a alors tout le loisir de vous retrouver grâce à vos adresses IP publiques et de réclamer le manque à gagner en faisant jouer la clause d'audit inscrite, elle aussi, aux conditions générales d'utilisation. Elle lui offre en effet la possibilité de contrôler votre système d'information pour vérifier que les logiciels utilisés sont dûment payés.

Les petits logiciels gratuits peuvent ainsi coûter fort cher à des DSI qui en ignoraient jusqu'à l'existence car les grands éditeurs ne sont plus les seuls à développer leurs ventes par un nouveau canal : l'audit.

## **L'effort fait les forts**

Ces deux cas d'école montrent que la compréhension des contrats de licences est indispensable pour éviter des complications désagréables. C'est par ailleurs un préalable à la gestion des actifs logiciels (Software Asset Management, SAM). Comment, en effet, maîtriser le droit d'usage contractuel d'un produit dont on ignore le contrat ?

En ces temps de crise, la chasse au manque à gagner est ouverte pour de nombreux éditeurs. Tout changement impliquant l'informatique concerne forcément des composants logiciels. Il convient donc d'être prudent et de prendre en considération leur dimension contractuelle. Bien des projets ont vu leur retour sur investissement réduit à néant, voire inversé, après un audit d'éditeur.

En définitive, qu'il s'agisse d'adopter le BYOD, d'utiliser un freeware ou de transformer le système d'information, le SAM renforce la position du client face aux éditeurs de logiciels car, comme disait Marcel Pagnol : « Comme on est faible quand on est dans son tort ! »... [Lire la suite]



Réagissez à cet article

# Les TPE et les PME, cibles privilégiées des cybercriminels | Denis JACOPINI



Les TPE et les PME, cibles privilégiées des cybercriminels

**Selon le spécialiste de la sécurité Symantec, 71 % des TPE et les PME qui font l'objet d'une cyber-attaque ne s'en remettent pas. Pourtant, la sécurité du système informatique ne fait pas partie des priorités des petites et moyennes entreprises, même si c'est un enjeu majeur pour leur survie.**

Face à des systèmes d'information de plus en plus ouverts, un usage généralisé d'internet et des terminaux mobiles connectés, les entreprises doivent mettre en œuvre des politiques de sécurité informatique de plus en plus exigeantes. Pourquoi les cybercriminels s'en prennent d'avantage aux TPE et aux PME ? Explication.

La cybercriminalité n'est pas un fait nouveau. Pourtant depuis quelques années, nous sommes tous devenus ultra-connectés et multi-équipés. Ce constat n'épargne pas les entreprises qui ont vu apparaître de nouveaux outils qui permettent aux salariés de rester connectés en étant plus mobile et plus productif. Ces nouveaux modes de travail, sont aujourd'hui autant de failles de sécurité possibles et donc d'attaques possibles. Cette forme de criminalité ne concerne plus les grandes entreprises qui ont majoritairement mis en place des moyens coûteux pour lutter contre le piratage. La nouvelle cible privilégiée des hackers serait les TPE et les PME qui seraient plus simple à attaquer.

#### **Des cibles plus accessibles**

Les enquêtes le confirment : les gérants de TPE et PME ont une vision assez exacte du piratage informatique, mais ils se sentent peu concernés. Selon eux, cette forme moderne de criminalité menace surtout les grandes entreprises. Pourtant, les délits constatés contredisent cette perception. Plus encore, le pourcentage des attaques vers les entreprises de moins de 250 salariés progressent. Selon le rapport Symantec Security Threat, elles seraient passées de 18% à 31% en 4 ans. Or ce sont justement les entreprises de moins de 250 salariés qui doivent protéger leurs données. Le constat est le suivant : 40% de la valeur des entreprises est issue des informations qu'elles détiennent. Ce qui intéresse les cybercriminels : dossiers clients, listes de contacts, renseignements sur le personnel et informations bancaires de l'entreprise, cartes de crédit comprises et propriétés intellectuelles. Elles représentent aussi des passerelles d'accès à leurs partenaires.

#### **Un frein pour travailler avec les grandes entreprises**

Loin des considérations financières et ne se sentant pas concernées, les TPE et PME s'estiment à l'abri de ces attaques. En conséquence, leurs infrastructures ne sont pas adaptées. Elles sont alors des cibles idéales permettant d'attaquer leurs différents partenaires qui sont parfois des grandes entreprises ou des administrations. Elles deviennent alors un moyen d'accéder à leurs systèmes d'information. Et cela peut constituer un frein à la compétitivité. Les Grandes Entreprises, ne pouvant contrôler le système d'information de leurs partenaires, exigent alors de leurs sous traitants un matériel informatique similaire afin de contrôler les flux.

#### **Des attaques virales invisibles**

Les attaques les plus fréquentes sont de natures virales. A l'insu des utilisateurs, elles visent à installer de petits programmes capables d'identifier les mots de passe (via des enregistreurs de frappe), d'accéder aux services bancaires en ligne de l'entreprise (Chevaux de Troie bancaires), de contrôler à distance les ordinateurs de l'entreprise pour lancer des attaques commandées (réseaux de zombies ou botnet) ou d'espionner les employés pour connaître leurs habitudes, leurs mots de passe ou leurs préférences (Spyware)...

#### **De nouvelles attaques plus structurées**

Les techniques de piratages évoluent et le matériel n'est plus l'unique faille. On voit apparaître de nouveaux types d'attaques basées sur les failles humaines et sociales. Les environnements de travail des salariés sont ciblés à travers les postes de travail des salariés. A titre d'exemple, les hackers identifient le lien entre les entreprises et leurs partenaires. Des mails sont envoyés depuis les réseaux sociaux type LinkedIn ou Viadeo au nom du partenaire. L'email sera donc ouvert sans réel méfiance de la part du salarié. Cette technique, appelée « social engineering », permet alors au pirate d'accéder au poste de travail de l'utilisateur en premier lieu pour ensuite évoluer dans le système d'information de l'entreprise.

#### **Des règles simples de cyber-stratégie**

Il n'est pas rare qu'en entreprise les salariés utilisent des outils réservés aux particuliers. Ce type de pratique multiplie les dangers d'intrusion car les systèmes peuvent être piratés. Ils pointeront vers l'installation de « maliciels » (logiciels malveillants conçus pour infiltrer un ordinateur et y réaliser des activités non autorisées). Il en est de même pour tous les outils connectés. Malheureusement, ce n'est souvent qu'une question de temps avant qu'un hacker arrive à ses fins. Il est donc primordial de faire preuve de plus de rigueur pour gagner du temps afin de décourager l'intrusion. Une entreprise qui connaît les risques et montre qu'elle a pris des mesures de sécurité simples, décourage les pirates. Il existe aujourd'hui des services de sécurité informatiques adaptés aux TPE/PME. A titre d'exemple, des prestataires proposent des offres sous forme de machine virtuelle, un proxy complet et simple. Le service permet de filtrer les pages internet en se basant sur des listes préétablies.

Mais bien avant de se consacrer à la sécurisation du matériel de travail, la première mesure à prendre concernera celle des bonnes pratiques des salariés. Des mesures de protection humaines sont nécessaires. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PricewaterhouseCoopers, spécialiste de la cyber sécurité. Le gouvernement met à disposition un Guide d'Hygiène et de Sécurité de l'ANSSI, il fournit les bases de la sécurité pour les utilisateurs au sein des entreprises.

Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :

- Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
- Définir les règles de prudence à appliquer au quotidien par l'entreprise et son personnel,
- Mettre en œuvre systèmes de protection électroniques adéquats. Le tout devant être organisé et planifié dans la durée.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

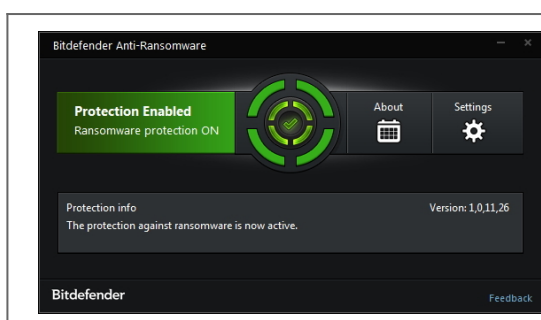
Un avis ? Laissez-nous un commentaire !

Source : <http://www.axione-limousin.fr/actualites/tpe-et-pme-cibles-privilegiees-des-cybercriminels-57.xhtml>



---

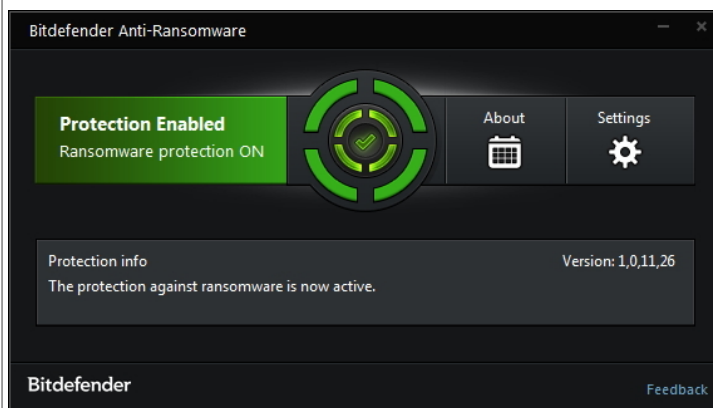
# Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ? | Denis JACOPINI



Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ?



Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.



Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.

The new Bitdefender Anti-Ransomware vaccine is built on the same principle as a previous tool that the company designed to prevent CryptoWall infections. CryptoWall later changed the way in which it operates, rendering that tool ineffective, but the same defense concept still works for other ransomware families.

While security experts generally advise against paying ransomware authors for decryption keys, this is based more on ethical grounds than on a perceived risk that the keys won't be delivered.

In fact, the creators of some of the most successful ransomware programs go to great lengths to deliver on their promise and help paying users decrypt their data, often even engaging in negotiations that result in smaller payments. After all, the likelihood of more users paying is influenced by what past victims report.

Many ransomware creators also build checks into their programs to ensure that infected computers where files have already been encrypted are not infected again. Otherwise, some files could end up with nested encryption by the same ransomware program.

The new Bitdefender tool takes advantage of these ransomware checks by making it appear as if computers are already infected with current variants of Locky, TeslaCrypt or CTB-Locker. This prevents those programs from infecting them again.

The downside is that the tool can only fool certain ransomware families and is not guaranteed to work indefinitely. Therefore, it's best for users to take all the common precautions to prevent infections in the first place and to view the tool only as a last layer of defense that might save them in case everything else fails.

Users should always keep the software on their computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. They should never enable the execution of macros in documents, unless they've verified their source and know that the documents in question are supposed to contain such code.

Emails, especially those that contain attachments, should be carefully scrutinized, regardless of who appears to have sent them. Performing day-to-day activities from a limited user account on the OS, not from an administrative one, and running an up-to-date antivirus program, are also essential steps in preventing malware infections.

« While extremely effective, the anti-ransomware vaccine was designed as a complementary layer of defense for end-users who don't run a security solution or who would like to complement their security solution with an anti-ransomware feature, » said Bogdan Botezatu, a senior e-threat analyst at Bitdefender, via email... [Lire la suite]



Réagissez à cet article

Source : *Free Bitdefender tool prevents Locky, other ransomware infections, for now | Computerworld*

---

# Comment vérifier si votre site Internet a été victime d'un Hackeur | Denis JACOPINI



Que ça soit à cause d'une simple erreur de frappe ou du fait que votre site Internet a été Hacké, l'auteur, l'éditeur ou le rédacteur en chef d'un site Internet peut être pénalement responsable des conséquences causées par son contenu non désiré.

Afin de vérifier si votre site Internet a été Hacké, voici quelques conseils pour vérifier si votre site Internet a été victime d'un Hackeur :

Que votre site Internet ait été victime d'un hackeur ou que votre site Internet ait été victime d'un pirate sont deux choses différentes.

Le pirate va pomper une partie ou la totalité du contenu de votre site Internet. Le hackeur va modifier le contenu de votre site Internet dans un but de malveillance.

Les conseils que je vais vous donner concernent le cas où un site Internet a été Hacké.

### **DU CONTENU ETRANGE APPARAIT ?**

En premier lieu, consultez votre site Internet sur plusieurs ordinateurs ayant des systèmes d'exploitation et des navigateurs différents afin de vérifier si un affichage anormal apparaît.

### **UN ANTIVIRUS DECLENCHE UNE ALERTE A L'OUVERTURE DE VOTRE SITE INTERNET ?**

Un message d'alerte de votre antivirus est aussi un bon indicateur de la présence éventuelle d'un code suspicieux sur votre site Internet.

Première solution : Depuis votre dernière sauvegarde vous n'avez plus fait de modifications :

Restaurez les pages Web ou la base de donnée contaminée.

Seconde solution : Vous n'avez pas de Sauvegarde de votre site Internet ou la sauvegarde est trop vieille :

Dans ce cas, vous allez devoir résoudre le problème à la main.

### **COMMENT TESTER VOTRE SITE INTERNET**

Enfin, si vous ne savez pas si votre site Internet a été hacké, vous pouvez le vérifier en utilisant les outils suivants :

<https://www.virustotal.com/url>

VirusTotal est un service gratuit qui *analyse les fichiers et URL suspects*, et facilite la détection rapide des virus, vers, trojans et tous types de malwares.

<http://www.urlvoid.com>

URLVoid.com is a free service developed by NoVirusThanks Company Srl that allows users to scan a website address with multiple website reputation engines and domain blacklists to facilitate the detection of possible dangerous websites, used to distribute malware and spyware or related to fraudulent activities.

<http://urlquery.net>

Query.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

<http://wepawet.iseclab.org/>

Dans ce cas, vous allez devoir résoudre le problème à la main.

### **COMMENT SE PROTEGER D'UN HACKEUR ?**

Voici quelques astuces simples vous aideront a protéger votre site efficacement contre les pirates et hackers de l'internet :

Ces techniques sont efficace contre les hackers débutants.

- Avoir un hébergeur de qualité et lui même utilisant des surveillances automatiques et permanentes.
- Mettez à jour systématiquement le système d'exploitation de votre serveur ainsi que toutes les applications liées à l'hébergement des sites internet, du FTP, des messageries et des bases de données.
- Supprimer l'utilisateur « admin » des logiciels et créez

le votre

- Mot de passe sécurisé (minuscules, majuscules, chiffres et symboles)

**Cet article vous à plu ? Laissez-nous un commentaire  
(notre source d'encouragements et de progrès)**

---

# **Se mettre en conformité avec la CNIL. Quel est le rôle de l'audit ? | Denis JACOPINI**

Notre métier en RGPD et en CYBER : Auditer, Expertiser,  
Accompagner, Former et Informer



---

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations [ici](https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd) : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

---

MISES EN CONFORMITÉ



PROTECTION  
DES  
DONNÉES PERSONNELLES

**CNIL**

Se mettre en  
conformité avec la  
CNIL. Quel est le  
rôle de l'audit ?

Depuis le 6 janvier 1978, les établissements public ou privés, les associations, les entreprises etc. doivent se mettre en conformité avec la Loi Informatique et Libertés. Un règlement européen entrant dans quelques mois en vigueur risquant de responsabiliser et sanctionner bien plus lourdement les concernés, il nous semblait important de vous détailler les étapes indispensables pour se mettre en conformité avec la CNIL.

Art. 226-16 de la Loi Informatique et Libertés

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés.

Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données, l'**#audit CNIL**, indépendant de la démarche de contrôle de la CNIL.

> Comment se passe un contrôle de la CNIL

Une fois cet **audit CNIL** réalisé, l'établissement connaissant enfin les actions qu'il doit mener va pouvoir prévoir deux actions de formation entrant dans notre cursus :

#### Se mettre en conformité avec la CNIL, mode d'emploi

- sensibiliser le personnel de l'établissement en lui expliquant la raison d'une démarche de mise en conformité CNIL et le comportement qu'il se verra adopter pour favoriser cette action ;
  - former le futur correspondant CNIL (CIL) à devenir autonome en lui inculquant :
    - les notions clés et grands principes de la loi informatique et libertés ;
    - les principes de base en matière de sécurité des systèmes d'information ;
    - le traitement des demandes et les modalités d'instruction d'une plainte ;
    - les contrôles et les procédures de sanction de la CNIL
  - La mise en application de la mise en conformité sur des cas concrets sur le système informatique de votre entreprise.
- Au terme de ces démarches, un nouvel **audit CNIL** peut être réalisé afin de vérifier la conservation de la conformité dans le temps.



Intéressé par une démarche de mise en conformité avec la CNIL ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

**Notre métier** : Denis JACOPINI est Expert indépendant, Expert judiciaire en Informatique spécialisé en protection des données personnelles. Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Nous pouvons également vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel. Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Sources : Denis JACOPINI

<https://www.cnil.fr/fr/comment-se-passe-un-contrôle-de-la-cnil>



---

# Mise en place d'un système de vote électronique, quelques conseils | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

✘

✘

✘

✘

✘

✘

✘

**Mise en place d'un système de vote électronique, quelques conseils**

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que tout système de vote électronique doit faire l'objet d'une expertise indépendante.

---

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises.

La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s'agit d'élections syndicales ou politiques.

La CNIL souligne que le recours à de tels systèmes doit

s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin (sauf pour les scrutins publics), le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement.

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que **tout système de vote électronique doit faire l'objet d'une expertise indépendante.**

Par ailleurs, l'article R2314-12 du Code du Travail créé par Décret n°2008-244 du 7 mars 2008 – art. (V) fixe très clairement que préalablement à sa mise en place ou à toute modification substantielle de sa conception, **un système de vote électronique est soumis à une expertise indépendante.** Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Information complémentaire : Les articles R2314-8 à 21 et R2324-4 à 17 du Code du Travail indiquent de manière générale les modalités du vote électronique lors du scrutin électoral de l'élection des délégués du personnel et des délégués du personnel au comité d'entreprise.

Ces dispositions ont été complétées par la délibération 2010-371 de la CNIL du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote

électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération et notamment sur :

- le code source du logiciel y compris dans le cas de l'utilisation d'un logiciel libre,
- les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après),
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau,
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité ;
- Ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- Posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- Avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique

doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

---

[Réagissez à cet article](#)

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

---

**Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise**



---

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le**

### **vote électronique ;**

- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

---

Contactez-nous


---

<http://www.cnil.fr/les-themes/vie-citoyenne/vote-electronique/>  
<http://www.cnil.fr/documentation/deliberations/deliberation/delib/249/>

<http://infosdroits.fr/la-cnil-sanctionne-un-employeur-pour-defaut-de-securite-du-vote-electronique-pendant-une-election-professionnelle/>

---

# Qui peut le consulter le FAED (Fichier automatisé des empreintes digitales) ? | Denis JACOPINI

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Qui peut le consulter le #FAED (#Fichier automatisé des empreintes digitales) ?</h2>
--	--

Seuls les agents habilités des services de l'identité judiciaire de la police nationale et des unités de recherches de la gendarmerie nationale ont directement accès au FAED, pour procéder aux opérations d'identification.

Les officiers de police judiciaire et les agents des douanes sont destinataires des résultats de la consultation du fichier, dans le cadre de leurs enquêtes.

Le FAED peut également être consulté, sous certaines conditions, par les agents des organismes internationaux de police judiciaire et par ceux des services de police ou de justice d'Etats étrangers.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

[http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=A8D0FF1FEB6BB72CCAD5DFA090DF59F2?name=FAED+\(Fichier+automatis%C3%A9+des+empreintes+digitales\)+%3A+qui+peut+le+consulter+%3F&id=423](http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=A8D0FF1FEB6BB72CCAD5DFA090DF59F2?name=FAED+(Fichier+automatis%C3%A9+des+empreintes+digitales)+%3A+qui+peut+le+consulter+%3F&id=423)

---

## Quelques conseils pour surfer

# un peu plus tranquille sur Internet

✖	Quelques conseils pour surfer un peu plus tranquille sur Internet
---	---

---



Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

## Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour**.

## Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu (firewall)** assureront un niveau de protection minimum pour surfer sur la toile. Le **firewall** permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

## Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

## Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence !**

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le *phishing*) ou de **pièces jointes piégées**. **Un simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant** (cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative**.

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

## Que faire si j'ai déjà cliqué sur la pièce jointe?

**Déconnectez-vous d'internet** et **ouvrez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :



---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Conseils de prévention sur

Internet / Cybercrime / Dossiers / Actualités – Police  
nationale – Ministère de l'Intérieur