# L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale | Nous pouvons vous aider à vous mettre en conformité | Denis JACOPINI

| | |
|---|---|
| | L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale | Nous pouvons vous aider à vous mettre en conformité |

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale.

*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. 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.

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI
Illustration : http://claudinelepage.eu/?p=8261

---

# Anti-phishing, Anti-Malware et protection des transactions bancaires pour ce logiciel de sécurité | Denis JACOPINI

#Anti-phishing, #Anti-Malware, et protection des transactions bancaires pour ce logiciel de sécurité

**Maintes fois récompensées par les critiques et les bêta-testeurs, les Editions 2016 des solutions de sécurité ESET sont enfin disponibles. Au programme, de nouvelles interfaces entièrement repensées et un nouvel outil pour sécuriser les transactions bancaires sur ESET Smart Security 9.**

En plus des technologies indispensables comme l'**anti-phishing** (pour **se protéger des e-mails de phishing**) et l'**anti-malware** (pour **se protéger des malwares cachés dans des e-mails ou des sites internet infectés**) qui protègent les clients contre les menaces d'Internet, ESET Smart Security 9 contient une toute nouvelle protection des transactions bancaires. Cette fonction met à disposition l'ouverture d'un navigateur sécurisé pour veiller à ce que toutes les transactions financières en ligne soient effectuées en toute sécurité. L'utilisateur peut également paramétrer lui-même tous les sites bancaires de paiement en ligne qu'il consulte le plus fréquemment.

---

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :

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

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.tuitec.com/face-a-la-hausse-des-cyberattaques-en-tunisie-eset-lance-ses-nouvelles-solutions/

---

# GDPR compliance: Request for costing estimate

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


# GDPR compliance: Request for costing estimate

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence.
Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best meet your needs.
Thus, we can assist you in bringing your structure into compliance in several ways : :
1. Are you looking for autonomy ?
We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support;
At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.
2. Do you want to be accompanied for the implementation of compliance ?
We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated;
At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).
3. Do you want to entrust all of your compliance?
In a perfectly complementary way with your IT service provider and possibly with your legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations relating to the protection of Personal Data.
From the audit to the follow-up, you can count on our technical and educational expertise so that your establishment is supported externally.
In order to send you a personalized proposal adapted both to the needs of your structure, in accordance with your strategy and your priorities, we would like you to answer these few questions :

**We guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to professional secrecy.**

---

Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations.

---

Your First Name / NAME (required)

Your Organization / Company (required)

---

Your email address (required)

---

A telephone number (will not be used for commercial prospecting)

---

You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below.

In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly.

## YOUR ACTIVITY

Details about your activity :
Are you subject to professional secrecy? OYes⊕NoOI don't know
Does your activity depend on regulations? OYes⊕NoOI don't know
If "Yes", which one or which ones?

## YOUR COMPUTER SYSTEM

Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .
Examples :
- 1 WEB server with website to publicize my activity;
- 1 desktop computer with billing software to bill my clients;
- 2 laptops including:
> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...
> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;
- 1 smartphone with email software to correspond with customers and prospects.

Do you have one or more websites? OYes⊕NoOI don't know
What is (are) this (thoses) website (s)?
Do you have data in the Cloud? OYes⊕NoOI don't know
Which cloud providers do you use?

## YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?

## SIZING YOUR BUSINESS

Number of employees in your structure : 0
How many of these employees use computer equipment ? 0
Number of departments or departments ** in your structure (example: Commercial service, technical service ...) : 0
Please list the services or departments ** of your structure:

## SERVICE PROVIDERS & SUBCONTRACTORS

Do you work with sub-contractors? OYes⊕NoOI don't know
Please list these subcontractors :
Do you work with service providers who work on your premises or in your agencies (even remotely) ? OYes⊕NoOI don't know
Please list these providers :
How many IT companies do you work with ? 0
Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :

## YOUR SITUATION TOWARDS THE GDPR

Does your establishment exchange data with foreign countries ? OYes⊕NoOI don't know
If "Yes", with which country(ies)?
Have you already been made aware of the GDPR ? OYes⊕NoOI don't know
Have people using IT equipment already been made aware of the GDPR ? OYes⊕NoOI don't know
If you or your employees have not been made aware of the GDPR, would you like to undergo training ? OYes⊕NoOI don't know

## YOUR WORKPLACE

The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.
Do you have several offices, agencies etc. legally dependent on your establishment ? OYes⊕No
If "Yes", how much ? 0
In which city (ies) (and country if not in France) do you or your employees work ?

## TYPE OF SUPPORT DESIRED

We can support you in different ways.
A) We can teach you to become autonomous (training) ;
B) We can support you at the start and then help you become independent (support, audit + training) ;
C) We can choose to entrust us with the entire process of compliance (support) ;
D) We can accompany you in a personalized way (thank you to detail your expectations).
What type of support do you want from us (A / B / C / D + details) ?

## END OF QUESTIONNAIRE

If you wish, you can send us additional information such as:
- Emergency of your project;
- Any additional information that you deem useful to allow us to better understand your project.

Send entered informations

*Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de LeNetExpert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-États-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2010 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des « données à caractère hautement personnel » pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi semestriel. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD (Règlement Général sur la Protection des Données), à la loi n°78-17 dite «Informatique et Libertés» du 6 janvier 1978 et à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant Le Net Expert, Monsieur le Délégué à la Protection des Données – 1 les Magnolias – 84300 CAVAILLON par Recommandé avec accusé de réception. Enfin, sur le fondement des articles 131-13, 222-17, 222-18, 222-18-1, 322-12, 322-13, R-621-1, R-621-2, R-623-1, R-624-3, R-624-4, R 631-1 et R634-1 du code Pénal et l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse, votre adresse IP horodatée est également collectée.*

***Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.***

** = for example, commercial service, technical service, educational service, administrative and financial service ...

Δ

or send an email to rgpd[at]lenetexpert.fr

**Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.**

Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n ° 15845), as a compliance practitioner and trainer, I support you in all your procedures for compliance with the GDPR.

**« My goal is to provide all my experience to bring your establishment into compliance with the GDPR. »**

# Peut-on être licencié pour ce qu’on y a écrit dans les réseaux sociaux ? | Denis JACOPINI


## Peut-on être licencié pour ce qu’on y a écrit dans les réseaux sociaux ?

**Peut-on être licencié pour ce qu’on y a écrit dans les réseaux sociaux ?**

Oui.
Dans une affaire concernant trois salariés licenciés pour avoir dénigré leur hiérarchie sur Facebook, un Conseil des prud’hommes a considéré que les propos publiés sur le mur d’un des salariés étaient publics car accessibles aux « amis d’amis ».
Ces propos ont perdu leur caractère privé du fait qu’ils étaient accessibles à des personnes non concernées par la discussion.
Soyez donc vigilant lorsque vous publiez des commentaires sur un réseau social !

---

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 : https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=D48813C492DFE134132210B5E195173E?id=199&back=true

# 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 liée 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.

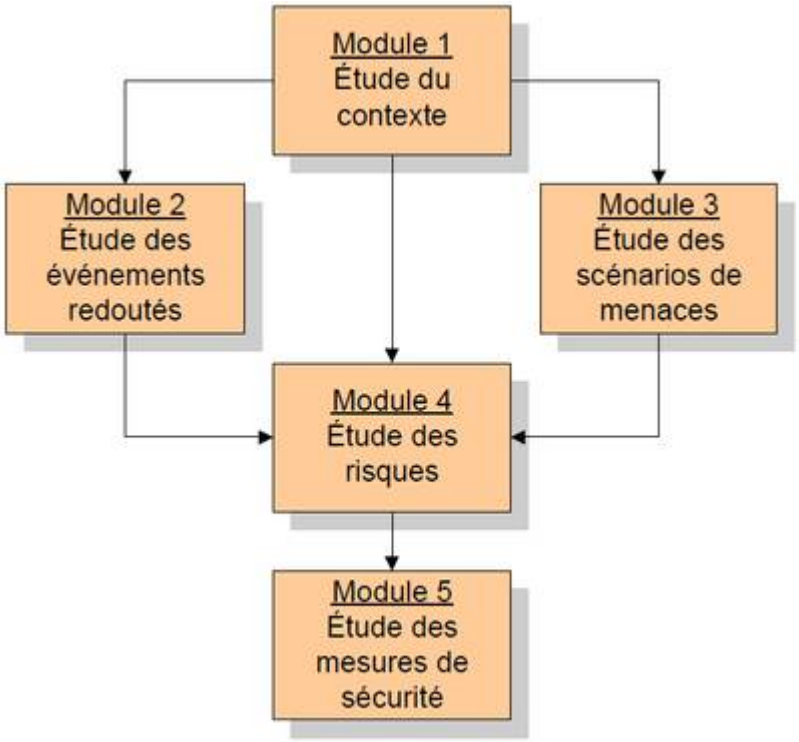
Contactez-nous

## 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 choisis-t-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 mesurer 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 connait 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 *spams* 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 | Divulgation 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…)… | Influençable (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 | *Man in the middle* 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

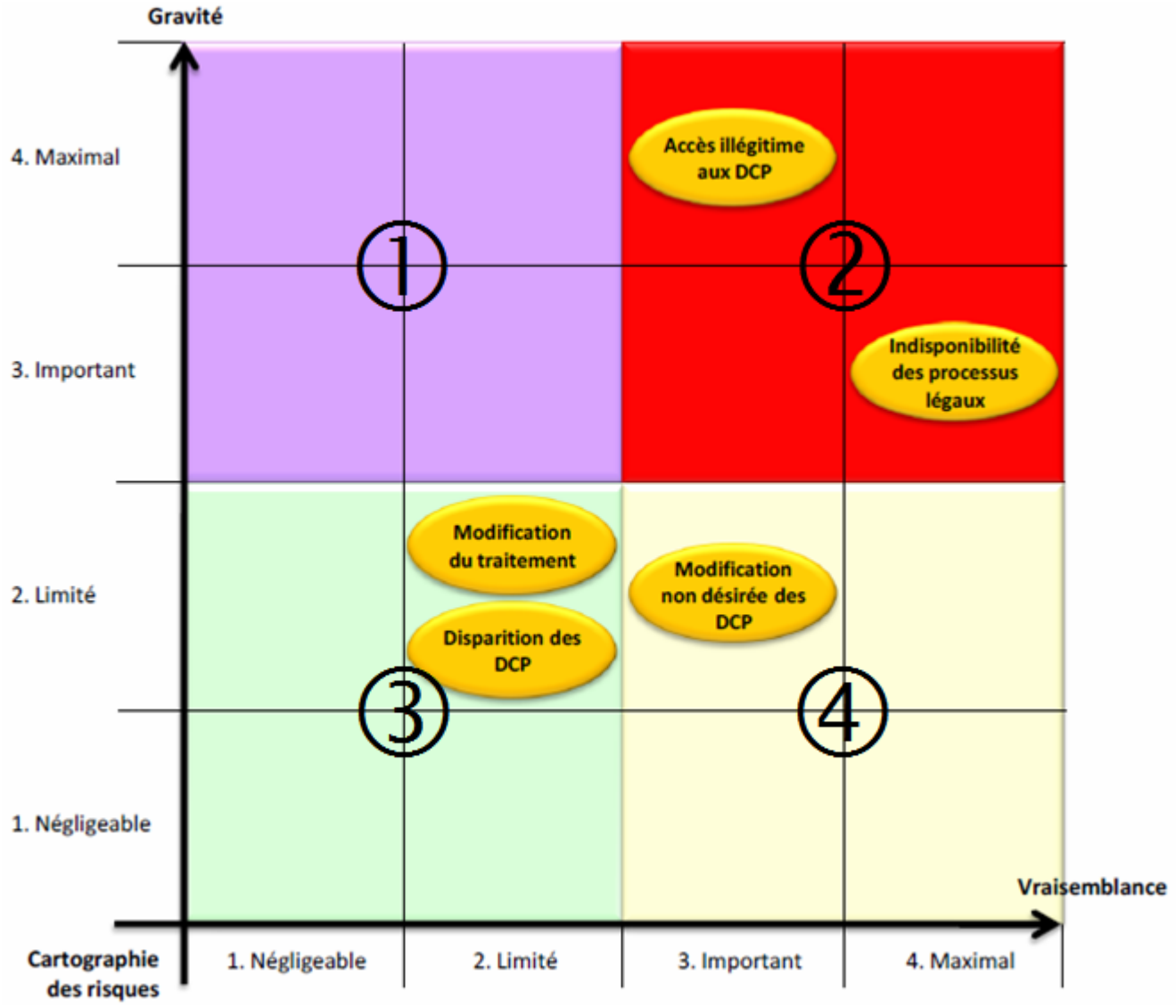
| Menaces génériques | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|
| D01. Détournement d'usage d'un matériel | Stockage de fichiers personnels, utilisation à des fins personnelles... | Utilisable en dehors de l'usage prévu... |
| D02. Dépassement des limites de fonctionnement 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 | Vieillissement 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 :

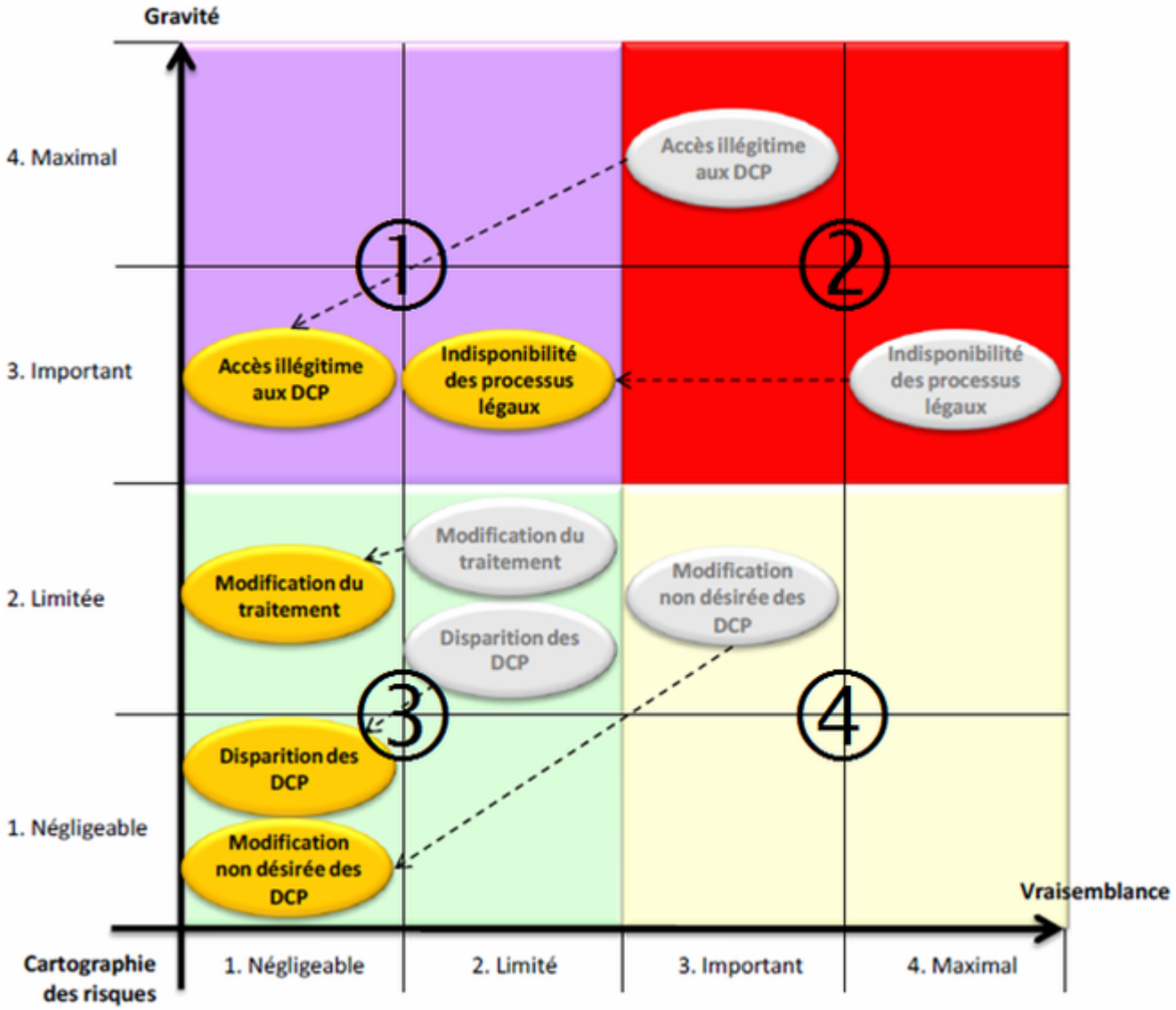
1. sur les éléments à protéger : mesures destinées à empêcher que leur sécurité ne puisse être atteinte, à détecter leur atteinte ou à recouvrer la sécurité informer les personnes concernées, minimiser les DCP, anonymiser les DCP…) ;
2. puis, si ce n’est pas suffisant, sur les impacts potentiels : mesures 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.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.

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

# RGPD : Que se passe t-il si le 25 mai 2018 nous n’avons pas terminé notre mise en conformité ?

RGPD : Que se passe t-il si le 25 mai 2018 nous n’avons pas terminé notre mise en conformité ?

**Le Net Expert : Denis JACOPINI, vous êtes spécialisé dans l'accompagnement des PME dans la mise en conformité avec le RGPD depuis plusieurs années. Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité avec le RGPD ?**

Si le 25 mai 2018 vous n'avez pas terminé votre mise en conformité avec le RGPD ou pire, vous venez à peine de l'initier pour votre entreprise, association ou administration, stricto sensu, en tant que responsable de traitement pénalement responsable, vous devenez amendable et les sanctions encourues, forcément pécuniaires selon les cas, pourraient être accompagnées de peines de prison comme le précise l'article 226-17 du Code pénal.
Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout État membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.
En réalité, avant que soient engagées des sanctions à votre encontre, vous serez contacté par la CNIL, laquelle vous demandera certainement de justifier les mesures prises à l'égard du Règlement Européen. Il est clair qu'au plus vous faites preuve de négligence, de mauvaise foi et de résistance, les sanctions risquées se rapprocheront du maximum à savoir la plus grande valeur entre 4% de votre chiffre d'affaire mondial ou 20 millions d'euros.
Si par contre, vous avez entamé une démarche de mise en conformité à savoir au minimum commencé à suivre une formation, désigné officiellement une personne (interne ou externe à votre entreprise) à cette démarche réglementaire et même si vous en êtes seulement au stade où vous avez commencé à établir la liste de vos traitements avec les risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel et si possible vous avez commencé à mettre en place des mesures correctives, vous montrerez ainsi à l'autorité administrative indépendante de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre organisation, pris au sérieux des défaillance en matière juridique ou technique de votre organisation et que des améliorations sont en cours. L'ensemble des démarches accomplies même après le 25 mai 2018 joueront en votre faveur en anéantissant les risques de sanction, bien évidemment à condition que vous ne fassiez aucune victime en cas de fuite de données avant.

---

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

---

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
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
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
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)

---

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

---

Réagissez à cet article

Source : Denis JACOPINI (Expert Informatique spécialisé RGPD)

---

# La cybercriminalité, un vrai risque pour les chefs d'entreprises | Denis JACOPINI

## La cybercriminalité, un vrai risque pour les chefs d'entreprises

**Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages.**
**Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises.**

Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours…) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable.La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau…). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.
Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise.
Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans l'entreprise.

---

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 protection juridique du chef d'entreprise.
Contactez-nous

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : Denis JACOPINI

# Comment se protéger du virus Dridex contenu dans les e-mails piégés | Denis JACOPINI


## Comment se protéger du virus Dridex contenu dans les e-mails piégés

**Après un mois d'interruption seulement, l'un des logiciels malveillants les plus virulents de 2015 fait son retour en France : plusieurs vagues d'envois massifs de courriels contenant le virus Dridex ont été constatées ces derniers jours. Ce malware de type « cheval de Troie » s'installe sur les ordinateurs Windows par le biais de pièces jointes piégées, dans le but de voler des coordonnées bancaires.**

**D'où vient ce virus ?**

Identifié dès juillet 2014 et repéré dans au moins 26 pays, Dridex n'a jamais vraiment disparu. Pourtant, fin août, une opération internationale coordonnée par le FBI et Europol (E3C), les agences de sécurité américaine et européenne, aboutissait à l'arrestation du Moldave Andreï Ghinkul, dit « Smilex », principal administrateur du virus. Les envois des courriels non-sollicités avaient été stoppés presque totalement le 2 septembre.

Mais le soulagement a été de courte durée : le 1er octobre, Palo Alto Networks détecte une nouvelle activité de Dridex au Royaume-Uni, puis le 14 octobre, c'est au tour de l'éditeur d'antivirus Avira d'émettre des doutes sur l'arrêt réel du botnet (réseau de serveurs et programmes destinés à propager le virus). Ce dernier paraît en effet toujours actif, selon Ayoub Faouzi, l'un des experts d'Avira.

Et effectivement, en France, le CERT-FR avertit le 23 octobre qu'une soixantaine de vagues d'envois massifs d'e-mails piégés visant la France ont eu lieu en moins de quinze jours.

Une nouvelle technique d'assemblage du code dite « just-in-time » (ou à la volée) permet aux pirates d'éviter les détections, mais aussi d'adapter plus rapidement le malware – une technique utilisée par d'autres logiciels malveillants comme GameOver Zeus.

**Comment fonctionne t-il ?**

Le mail reçu se présente de façon anodine : la plupart du temps, une relance de facture, incluant une pièce jointe au format. doc de Microsoft Office. À l'heure actuelle, peu d'antivirus détectent la nouvelle variante de ce logiciel (qui est signé avec un certificat officiel paraissant émaner de l'entreprise de sécurité Comodo), et la plupart ne suppriment donc pas la pièce jointe.

Si le destinataire tente d'ouvrir le document Word joint, une page vierge va s'afficher, mais le logiciel de Microsoft va tout de même demander à l'utilisateur s'il veut activer les macros (permettant d'interpréter les codes éventuellement contenus dans les documents Office). Une réponse positive active le virus et va lancer le téléchargement discret d'un premier code malicieux.

D'autres fichiers sont ensuite téléchargés afin d'installer divers programmes-espions. Il ne reste plus au pirate qu'à décider quand et quel programme utiliser et installer pour récupérer les données personnelles et bancaires puis effectuer des opérations frauduleuses.

**A quoi ressemblent ces e-mails piégés ?**

Les premières vagues de mails, le plus souvent intitulés « Relance Facture urgent » ou de « AR CDE + Facture Proforma », ont touché des messageries personnelles ou d'entreprises dès le mois de juin. Ecrits dans un français très correct et sans fautes d'orthographe, ces textes courts, et suffisamment sibyllins pour inquiéter ceux qui les reçoivent, ont déjà fait l'objet d'une première alerte officielle émanant du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. La nouvelle vague de mails reçus ces deux dernières semaines sont du même tonneau.

Exemples :

*« Objet : PIXOLUTIONS – FACTURE N°03480830-260615*

*Bonsoir,*

*Veuillez trouver en pièce jointe la facture n°03480830-260615 correspondant à la réalisation et pose du logo végétalisé à Perpignan. Vous en souhaitant bonne réception, bien cordialement, ».*

*« Objet : DUPLICATA FAC N°87878241*

*Salut,*

*Il parait que tu recherches la facture avec les Rimauresq Rosé et Blanc ? La voici en pièce jointe. Veux-tu que je te la remette au courrier également ? »*

*« Objet : Comptabilité de PACAR : facture n° 94352132 du 26/10 de 439,99 euros*

*Bonjour,*

*Pouvez-vous nous envoyer un chèque de 439,99 euros en paiement de la facture n° 94352132 dont vous trouverez la copie ci-jointe. En vous remerciant, Bien cordialement, »*

**Comment s'en protéger ?**

En plus d'un antivirus à jour, il est recommandé d'observer une grande vigilance à la réception de tout message contenant une pièce jointe, et ce quel que soit son format (.doc, .odt, .xls, .pdf, etc.).

Si le courriel semble émaner d'un organisme officiel (administrations, banques, boutiques en ligne, etc.), il est préférable de tenter de les contacter soit par téléphone, soit par mail pour vérifier l'objet de la correspondance et la légitimité de l'envoi.

Enfin, l'étape de sécurité optimale consiste à désactiver l'exécution automatique des macros dans les suites bureautiques de type Microsoft Office (aller dans Fichiers/Options/Centre de gestion de la confidentialité/Paramètre du Centre de gestion de la confidentialité/Paramètres des macros/Désactiver toutes les macros avec notifications).

**Comment vérifier sa présence et s'en débarrasser ?**

La société française de sécurité Lexsi propose un simple outil de détection permettant tout à la fois de vérifier sa présence sur un ordinateur puis de l'éradiquer complètement. Il est également possible, comme l'explique Lexsi, de nettoyer manuellement son ordinateur.

Téléchargez l'outil sur :
https://www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

---



---



Source : http://www.lemonde.fr/pixels/article/2015/10/29/e-mails-pieges-nouvelle-alerte-au-virus-dridex-en-france_4799355_4408996.html

# Le Crowdfunding, risques, pièges et précautions à prendre | Denis JACOPINI

Le Crowdfunding, désigne le financement participatif.Est-il risqué ?Quels sont ses pièges ?Quelles sont les précautions à prendre ?

# Les petites entreprises aussi victimes de cybercriminalité | Denis JACOPINI

**Vols 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 fraudes 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, ndlr). 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 audité, 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 cuite 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.

---



---



---



Source : http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri_1518760.html