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. »

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.

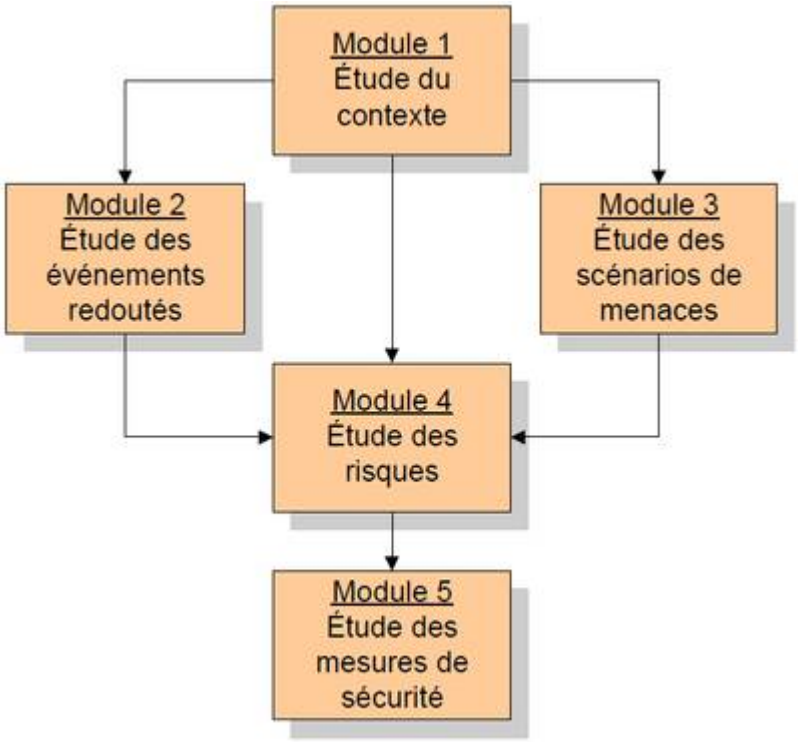
Contactez-nous

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

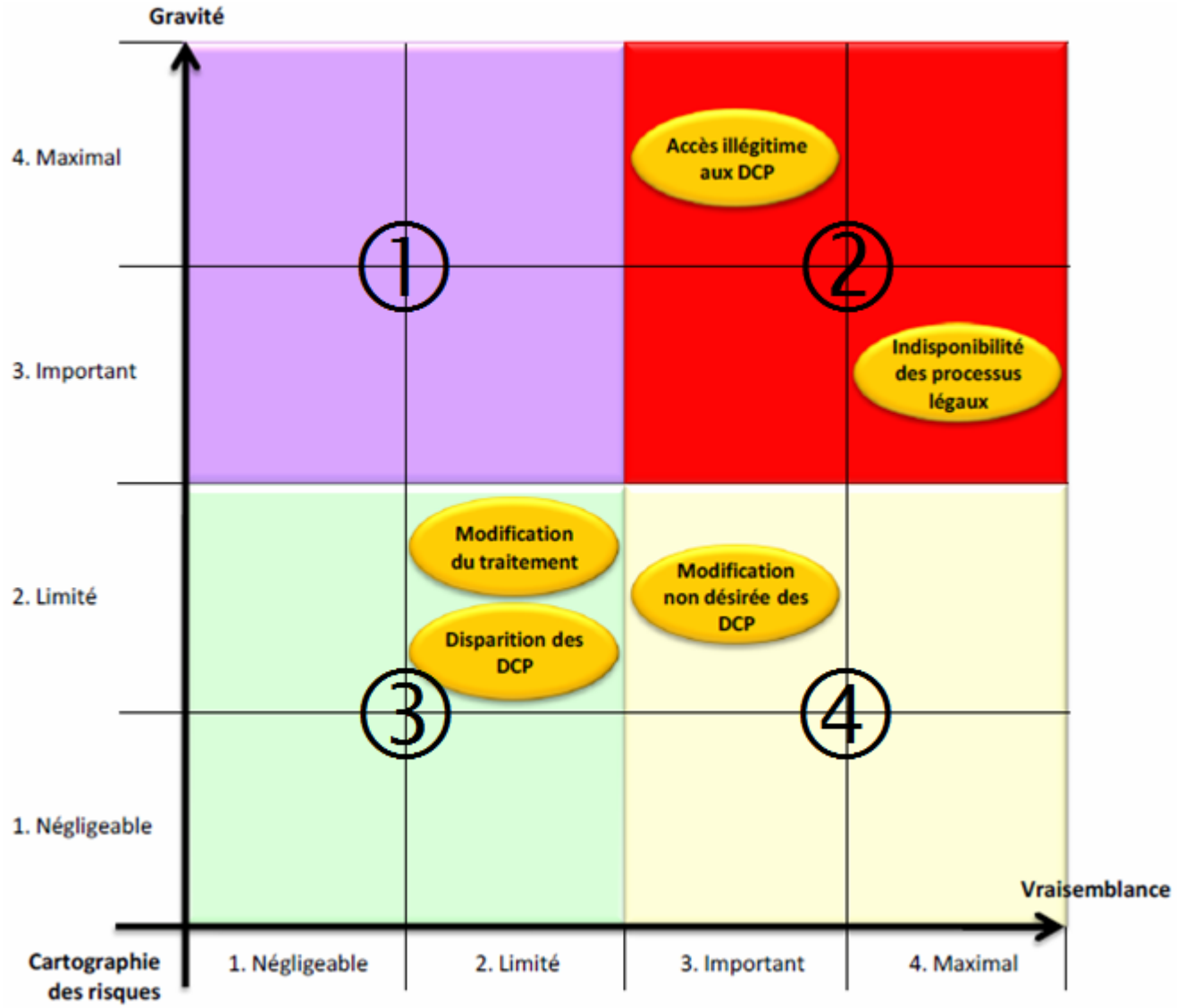
Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
D01. Détournement d'usage d'un matériel	Stockage de fichiers personnels, utilisation à des fins personnelles...	Utilisable en dehors de l'usage prévu...
D02. Dépassement des limites de fonctionnement d'un matériel	Unité de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

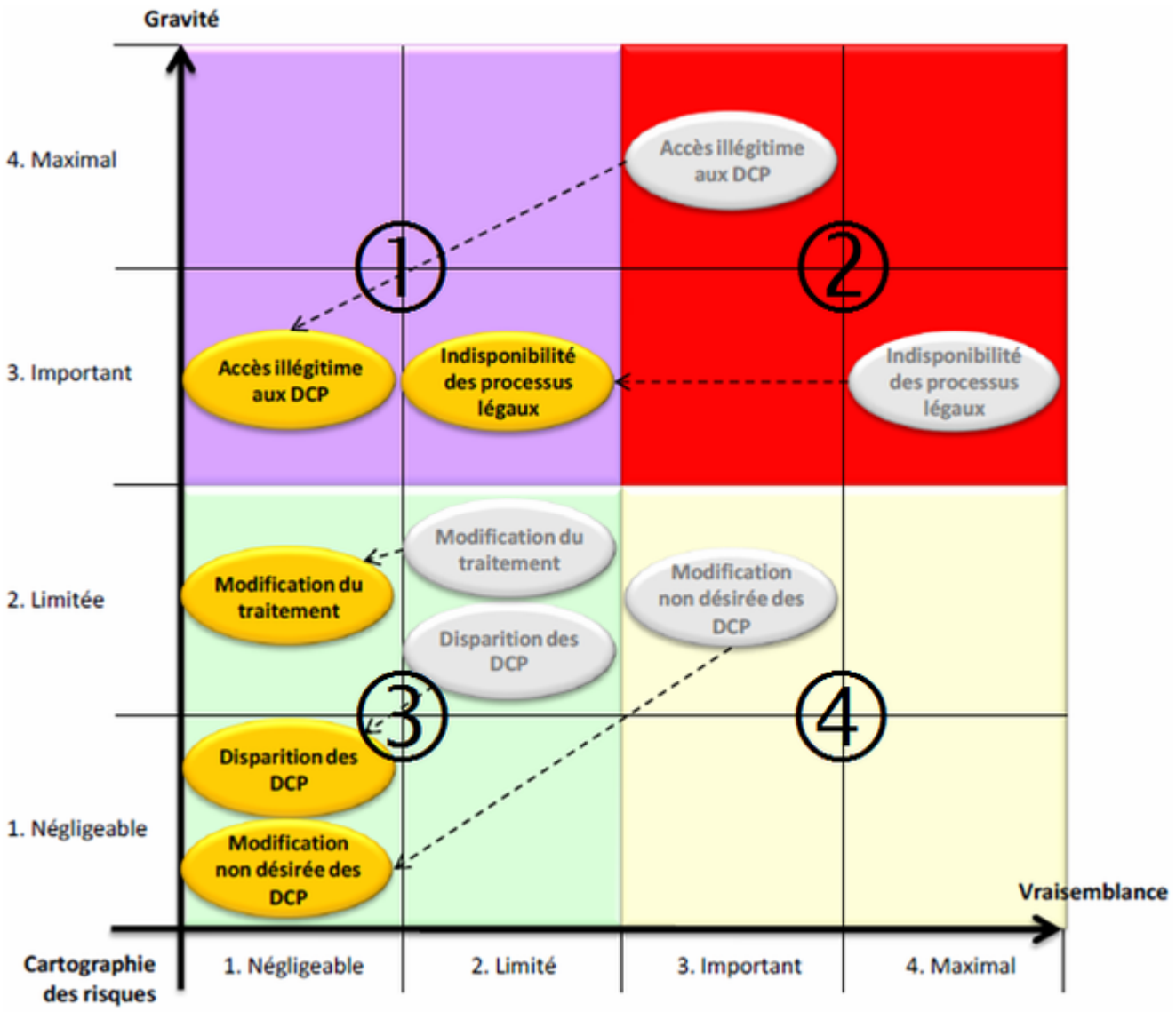
Cette action consiste à déterminer des mesures complémentaires qui vont porter :

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.

Contactez-nous

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

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 ?

Attaque informatique TV5 Monde – Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8 | Denis JACOPINI

	Attaque informatique TV5 Monde -Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8

A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable…- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

– Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux… Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les deffaçages de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.

Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

– la recherche de failles

– la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.

Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »

Peut-on conclure que n'importe quelle chaines de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaines de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

Existe t-il un moyen de se protéger contre ce type d'attaque ?

Les organismes et entreprises ont prix trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début…

http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4

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 : http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html

Procédure à suivre pour demander l’aide juridictionnelle | Denis JACOPINI

	Comment demander l’aide juridictionnelle Il vous semble qu’un logiciel espion se cache dans votre iphone, votre smartphone, votre ordinateur, ou votre téléphone ? Vous soupçonnez être victime d’espionnage informatique ? Vous souhaitez utiliser les services d’un #expert informatique pour faire analyser votre appareil ? Avant d’engager les services d’un expert informatique,vérifiez si vous n’avez pas droit à une prise en charge par l’état de vos frais juridiques.

Vous êtes ou il vous semble être victime d’espionnage de votre ordinateur, de votre téléphone ou de votre smartphone ?

Vous souhaitez utiliser les services d’un expert informatique pour faire analyser votre appareil ?

Vous pouvez probablement bénéficier de l’aide

juridictionnelle.

L’aide juridictionnelle, c’est quoi ?

L’aide juridictionnelle vous permet, si vous avez de faibles ressources, de bénéficier d’une prise en charge totale ou partielle par l’État des honoraires et frais de justice (avocat, huissier, expert, etc.).

Si la prise en charge par l’état est totale

Tous vos frais sont pris en charge, à l’exception du droit de plaidoirie fixé à **13 €** dû devant certaines juridictions et à payer à votre avocat.

Attention
Les sommes engagées avant la demande d’aide juridictionnelle ne sont pas remboursées.

Si la prise en charge par l’état est partielle

L’État ne prend en charge qu’une partie des honoraires d’avocat. Vous devez lui verser des honoraires complémentaires à fixer avec lui avant le procès.

Les autres frais relatifs aux instances, procédures ou actes pour lesquels l’aide juridictionnelle partielle vous a été accordée (frais d’expertise, d’enquête sociale, droit d’enregistrement, etc.) sont totalement pris en charge par l’État.

Remarque
L’aide juridictionnelle (totale ou partielle) ne couvre pas les frais auxquels vous pouvez éventuellement être condamné à l’issue du procès (condamnation aux dépens, dommages et

intérêts).

Comment demander l’aide juridictionnelle ?

Formulaire de demande d’aide juridictionnelle – Cerfa n°12467*01

Site Internet sur l’aide juridictionnelle du site Service-Public.fr

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

Références :

Loi n°91-647 du 11 juillet 1991 relative à l’aide juridique

Décret n°91-1266 du 19 décembre 1991 relatif à l’aide juridique

Arrêté du 23 novembre 2011 sur les procédures visées par le décret du 15 février 1995 relatif aux droits de plaidoirie

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 partir 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)

Utilisation des données personnelles dans le cas de la prospection Téléphonique – Rappel des règles | Denis JACOPINI

	Dans le cadre de vos activités, vous pouvez être amenés à contacter par téléphone des personnes. Quelles sont les règles à respecter ?

LE PRINCIPE : Information préalable et droit d’opposition.

La prospection par téléphone (télémarketing) est possible à condition que la personne soit, au moment de la collecte de son numéro de téléphone :

- informée de son utilisation à des fins de prospection.
- en mesure de s’opposer à cette utilisation de manière simple et gratuite, notamment par le biais d’une case à

cocher.

LÉGISLATION APPLICABLE

Article 38 de la loi Informatique et Libertés du 6 janvier 1978

Articles L.34 et R.10 du code des postes et des communications électroniques.

RÉFÉRENCES UTILES

Code Déontologique du e-commerce et de la vente à distance du FEVAD

SANCTIONS

Amende de 750 € par appel
dans le cas de l'utilisation des coordonnées des personnes inscrites sur la « Liste Orange », à partir des annuaires téléphoniques (contravention de la 4e classe prévue par l'article R.10-1 alinéa 1 du code des postes et des communications électroniques).

5 ans emprisonnement et 300 000 € amende
Délit prévu par les articles 226-18 et 226-18-1 du code pénal.

Jusqu'à 300 000 € d'amende
Sanction prononcée par la CNIL, prévue par l'article 47 de la loi informatique et libertés modifiée.

Cet article vous à plu ? Laissez-nous un commentaire

(notre source d’encouragements et de progrès)