Bonnes pratiques face à une tentative de cyber-extorsion | Denis JACOPINI

Bonnes pratiques face à une tentative de cyber-extorsion

Bonnes pratiques face à une tentative de cyber-extorsion

1. Typologie des différents cas de cyber-extorsion

Le type le plus répandu de cyber-extorsion est l'attaque par crypto-ransomware. Ce dernier est une forme de malware qui chiffre les fichiers présents sur la machine infectée. Une rançon est par la suite demandée afin d'obtenir la clef qui permet de déchiffrer les données compromises. Ces attaques touchent autant les particuliers que les acteurs du monde professionnel. Il existe cependant deux autres types de cyber-extorsion auxquels doivent faire face les sociétés.

Le premier cas est celui du chantage faisant suite à un vol de données internes. L'exemple le plus marquant de ces derniers mois est celui du groupe Rex Mundi : ce dernier dérobe des informations sensibles/confidentielles – comme une base clientèle – puis demande une rançon à sa victime sous peine de divulguer son butin et par conséquent de rendre public l'acte de piratage; ce qui peut être fortement compromettant pour la société ciblée comme pour sa clientèle. De nombreuses entreprises comme Dexia, Xperthis, Voo ou encore Labio ont été victimes des chantages du groupe Rex Mundi.

La deuxième pratique est celle du DDoS contre rançon, spécialité des pirates d'Armada Collective. Le modus operandi est simple et efficace : la cible reçoit un email l'invitant à payer une rançon en Bitcoin afin de ne pas se voir infliger une puissante attaque DDoS qui rendrait son site web indisponible à ses utilisateurs. La plupart des victimes sont des sociétés de taille intermédiaire dont le modèle économique est basé sur le principe de la vente en ligne – produits ou services – comme le fournisseur suisse de services de messagerie ProtonMail en novembre 2015.

2. Bonnes pratiques à mettre en place

En amont de la tentative de cyber-extorsion

Un ensemble de bonnes pratiques permet d'éviter qu'une attaque par ransomware se finalise par une demande de rançon.

Il convient de mettre en place une stratégie de sauvegarde – et de restauration – régulière des données. Ces back-ups doivent être séparés du réseau traditionnel des utilisateurs afin d'éviter d'être chiffrés en cas de déploiement d'un crypto-ransomware. Dans ce cas de figure, le système pourra être restauré sans avoir besoin de payer la rançon exigée.

La propagation d'un malware peut également être évitée par l'installation d'outils/solutions de cybersécurité notamment au niveau du client, du webmail et du système d'exploitation (antivirus). Ceci doit obligatoirement être couplé à une mise à jour régulière du système d'exploitation et de l'ensemble des logiciels installés sur le parc informatique.

L'être humain étant toujours le principal maillon faible de la chaîne, il est primordial de sensibiliser les collaborateurs afin qu'ils adoptent des comportements non-risqués. Par exemple : ne pas cliquer sur les liens et ne pas ouvrir les pièces-jointes provenant d'expéditeurs inconnus, ne jamais renseigner ses coordonnées personnelles ou bancaires à des opérateurs d'apparence légitimes (banques, fournisseurs d'accès Internet, services des impôts, etc.).

Ces bonnes pratiques s'appliquent également dans le cas d'un chantage faisant suite à un vol de données internes. Ces dernières sont en général dérobées via l'envoi dans un premier temps d'un spam contenant une pièce jointe malicieuse ou une URL redirigeant vers un site web compromis. Une fois le système d'information compromis, un malware est déployé afin de voler les informations ciblées.

La menace provient également de l'intérieur : un employé mal intentionné peut aussi mettre en place une tentative de cyber-extorsion en menaçant de divulguer des informations sensibles/confidentielles. Ainsi, il est important de gérer les accès par une hiérarchisation des droits et un cloisonnement.

Pendant la tentative de cyber-extorsion

Lors d'un chantage faisant suite à un vol de données internes, il est important de se renseigner sur la véracité des informations qui ont été dérobées. Certains groupes de pirates se spécialisent dans des tentatives de cyber-extorsion basées sur de fausses informations et abusent de la crédulité de leurs victimes. Il en va de même concernant l'origine du corbeau : de nombreux usurpateurs imitent le style du groupe Armada Collective et envoient massivement des emails de chantage à des TPE/PME. Ces dernières cèdent fréquemment à ces attaques qui ne sont pourtant que des canulars.

Il est vivement recommandé de ne jamais payer une rançon car le paiement ne constitue pas une garantie. De nombreuses victimes sont amenées à payer une somme bien plus conséquente que la rançon initialement demandée. Il n'est pas rare de constater que les échanges débutent de manière très cordiale afin de mettre la cible en confiance. Si cette dernière cède au premier chantage, l'attaquant n'hésite pas à profiter de sa faiblesse afin de lui soutirer le plus d'argent possible. Il abuse de techniques basées sur l'ingénierie sociale afin d'augmenter ses profits. Ainsi, l'escroc gentil n'existe pas et le paiement de la rançon ne fait que l'encourager dans sa démarche frauduleuse.

De nombreuses victimes refusent de porter plainte et cela pour plusieurs raisons. Elles estiment à tort que c'est une perte de temps et refusent également de communiquer sur les résultats et conséquences d'une attaque qui ne feraient que nuire à leur image auprès des clients, fournisseurs ou partenaires. Pourtant cette mauvaise stratégie ne fait que renforcer le sentiment d'impunité des attaquants, les confortent dans le choix de leurs modes opératoires et leur permet de continuer leurs actions malveillantes. Il est ainsi vital de porter plainte lors de chaque tentative de cyber-extorsion. L'aide de personnes qualifiées permet de faciliter ce genre de démarches.

En cas d'attaque avérée, il est essentiel pour la victime de s'appuyer sur un panel de professionnels habitués à gérer ce type de situation. La mise en place d'une politique de sauvegarde ou bien la restauration d'un parc informatique n'est pas à la portée de toutes les TPE/PME. Il est nécessaire de faire appel à des prestataires spécialisés dans la réalisation de ces opérations complexes.

Par ailleurs, en cas de publication de la part de l'attaquant de données sensibles/confidentielles, il convient de mettre en place un plan de gestion de crise. La communication est un élément central dans ce cas de figure et nécessite l'aide de spécialistes.

Article original de Adrien Petit

Réagissez à cet article

Original de l’article mis en page : Bonnes pratiques face à une tentative de cyber-extorsion [Par Adrien Petit, CEIS] | Observatoire FIC

Spécial Phishing 1/3 : Quelle est la technique des pirates informatiques ?

On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :

• cliquer sur une pièce-jointe ou un lien piégés
• communiquer des informations personnelles

2. L’attaquant se fait passer pour une personne ou un tiers de confiance

L’attaquant est alors en mesure de :

• prendre le contrôle de votre système
• faire usage de vos informations

3. Impact de l’attaque

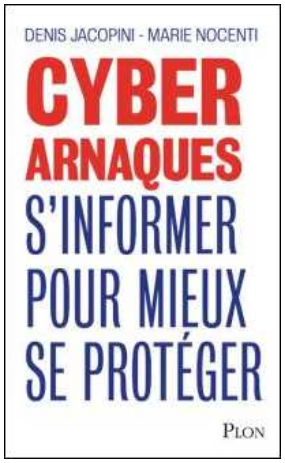
• Intégrité
• Authenticité
• Disponibilité
• Confidentialité

Motivations principales

• Atteinte à l’image
• Appât du gain
• Nuisance
• Revendication
• Espionnage
• Sabotage

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr
Source : *ANSSI – On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.*

Que faire si on vous refuse

l’accès à votre dossier médical ? | Denis JACOPINI


Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer
LE NET EXPERT
AUDITS & EXPERTISES
EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES
LENETEXPERT .fr
RGPD CYBER
LE NET EXPERT
MISES EN CONFORMITÉ
SPY DETECTION
Services de détection de logiciels espions
LE NET EXPERT
FORMATIONS
LE NET EXPERT
ARNAQUES & PIRATAGES

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

Que faire si on vous refuse l’accès à votre dossier médical ?

Vous avez demandé à avoir accès à votre dossier médical et vous n’avez pas eu de réponse ou une réponse négative ?
Si votre dossier est détenu par un hôpital public ou une clinique participant au service public hospitalier, adressez un courrier à la Commission d’accès aux documents administratifs :
CADA
35, rue Saint Dominique
75700 Paris 07 SP
Si votre dossier est détenu par un établissement privé (clinique) ou un médecin libéral (généraliste ou spécialiste), vous pouvez adresser une plainte à la CNIL.

Adresser une plainte à la CNIL

Vous pouvez également porter plainte auprès du procureur de la République du Tribunal de grande instance dont vous dépendez.

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

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

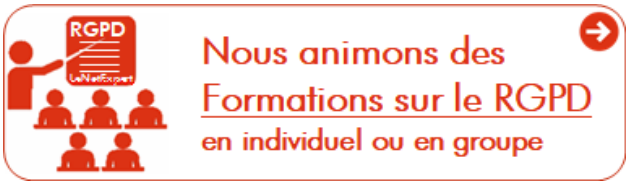
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

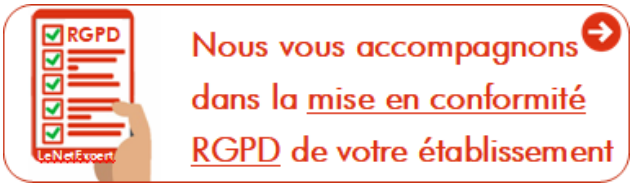
Contactez-nous

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=9DCFCE66E3DC38F485EA18F87E1E023F?name=Dossier+m%C3%A9dical+%3A+que+faire+si+on+me+refuse+l%27acc%C3%A8s+%3F&id=265

Elections par Internet et Votes électroniques

Les décrets d'application de la Loi Travail continuent d'arriver en ce dernier mois de l'année 2016. L'ultime en date concerne le vote électronique (1). En tant que représentants du personnel, que vous soyez délégué du personnel ou membre du comité d'entreprise, vous vous demandez quelles sont les conditions à réunir pour recourir à ce type de dispositif. Vous souhaitez savoir quels sont les apports de la Loi Travail sur le vote électronique : quel accord mettre en place et quelles garanties pour le système adopté ? Voici les 3 points essentiels à connaître à propos du vote électronique !

Avant la loi Travail, le vote électronique n'était possible que sous réserve d'avoir été prévu par un accord collectif. Mais est-ce toujours le cas ? Pour quelles élections peut-on recourir au vote électronique ? Quelles sont les garanties de régularité de ce vote ?

Les élections concernées par le vote électronique

Il est possible de recourir au **vote électronique** pour **deux élections** visées dans le décret du 5 décembre 2016 :

• les **délégués du personnel** ;

• les représentants du personnel au **comité d'entreprise**.

Sachez qu'il est d'ailleurs possible de combiner vote électronique et vote sous enveloppe, à condition que l'acte qui autorise le recours au vote électronique n'exclue pas cette possibilité *(2)*.

Les modalités du vote électronique

La mise en place du vote électronique est soumise à quelques formalités préalables. Ce recours doit être prévu dans un **accord de groupe** ou un **accord d'entreprise** (2).

Désormais, à défaut d'accord collectif, **l'employeur** peut **décider unilatéralement** de recourir au vote électronique *(2)*. C'est la nouveauté inscrite dans ce décret d'application de la loi travail.

Sachez aussi que le **protocole d'accord préélectoral**, qui doit être négocié entre l'employeur et les organisations syndicales représentatives, doit mentionner l'accord collectif ou la décision de l'employeur de recourir au vote électronique.

Quel est le contenu du protocole d'accord préélectoral ?

Lors de la négociation de ce protocole, il faudra tenir compte des contraintes techniques posées par ce vote particulier. En effet, comme tout dispositif électronique, des garanties doivent être prises pour assurer la **régularité du vote** et sa **confidentialité**.

A ce titre, le code du travail établit un **cahier des charges** à respecter :

• des **fichiers distincts** dans l'urne : il doit y avoir deux fichiers qui doivent être bien séparés. Le premier « **Fichier des électeurs** » doit permettre l'authentification des électeurs. Le second fichier nommé « **Contenu de l'urne électronique** » détaillera lui les clés de chiffrement et de déchiffrement, ainsi que le contenu de l'urne. Ce fichier n'est **consultable que par les personnes en charge de la gestion et de la maintenance du système de vote** *(3)*.

• le système de vote doit pouvoir être **scellé** pendant toute la durée du scrutin *(4)*.

• une **expertise indépendante** doit être réalisée **avant le scrutin***(5)* par un **expert indépendant** mandaté par l'employeur.

• une **assistance technique** doit être mise en place par l'employeur pour veiller au bon fonctionnement du système et intervenir en cas de besoin *(6)*. Des tests doivent être effectués sur le matériel avant le déroulement du vote.

Les garanties prévues pour la régularité du vote

Le vote électronique doit présenter certaines garanties indispensables à sa régularité :

• le **respect du cahier des charges** prévu par la loi.

Il est mentionné dans l'accord collectif ou la décision unilatérale de l'employeur de recourir au vote électronique.

Par ailleurs, **chaque salarié** doit avoir **accès à ce cahier des charges** selon le décret du 5 décembre 2016 *(2)*. Il peut être mis à leur disposition via l'intranet de l'entreprise ou consultable dans les locaux de l'entreprise.

L'expertise préalable par un expert indépendant.

Tout le système et le matériel de vote doit avoir été examiné par un expert rémunéré par l'employeur.

Il s'assure de l'existence de la **décision unilatérale de l'employeur** ou de l'**accord collectif** autorisant le recours au vote électronique.

Il doit s'assurer également des modalités garantissant la **confidentialité** et la **sécurité du dispositif** : l'existence des deux fichiers séparés concernant les électeurs et le contenu de l'urne, l'exclusivité de l'accès aux données électroniques par les gestionnaires du système, le caractère hermétique et scellé du matériel.

Il rédigera un **rapport** sur ces points. Ce dernier doit être tenu **à la disposition de la CNIL** *(7)*.

La déclaration à la CNIL.

Comme tout dispositif électronique et de stockage informatique de données, le vote électronique doit faire l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés *(8)*.

A ce titre, la CNIL a fait une recommandation relative à la sécurité des systèmes de vote électronique.

Lire la recommandation de la CNIL

Les **organisations syndicales représentatives de salariés** doivent être **informées de l'accomplissement de cette formalité** déclarative auprès de la CNIL.

Les résultats du vote.

Si l'acte qui autorise le recours au vote électronique n'a pas exclu le vote sous enveloppe à bulletin secret, sachez qu'il ne sera pas possible d'obtenir des premiers résultats pendant le scrutin. En effet, le récent décret précise bien qu'**aucun résultat partiel n'est accessible pendant le déroulement du vote**. L'ouverture des enveloppes ne pourra être faite qu'après la clôture du vote électronique *(9)*.

Pour aller plus loin dans vos démarches

Je me présente : Denis JACOPINI. Je suis Expert en Informatique indépendant et assermenté spécialisé en Cybercriminalité et en Protection des Données à Caractère Personnel répondant à l'ensemble des critères relatifs aux Experts recommandés par la CNIL en mesure de vous accompagner pour vos élections par voie électronique pendant toutes les phases suivantes :

1. AVANT ET HORS EXPERTISE (FACULTATIF)

– Analyse technique des réponses des éditeurs à la suite de votre appel d'offres ou consultation ;
– Présentation des résultats de l'analyse technique des réponses des éditeurs au bureau de vote ;
– Accompagnement pendant toute la phase de rencontre avec l'éditeur jusqu'à la recette du logiciel de vote électronique ;

2. DANS LE CADRE DE L'EXPERTISE

– Expertise préalable aux élections conforme à la délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique avec la possibilité d'ajouter dans notre expertise technique des contrôles relatifs à d'autres obligations, normes ou référentiels propres à votre activité professionnelle réglementée (Droit, Santé, Fiscal, Social…) ;
– Avis technique préalable à l'ouverture des scrutins ;
– Participation à la cérémonie de scellement des urnes (sur place en fonction de nos disponibilités sinon disponibilité à distance et possibilité de présence d'un tiers de confiance) ;
– Suivi de vos élections à distance de manière aléatoire ;
– Participation au dépouillement des urnes (sur place en fonction de nos disponibilités sinon disponibilité à distance et possibilité de présence d'un tiers de confiance) ;
– Avis technique à la suite de la clôture des scrutins ;
– Vérification de la suppression des données à caractère personnel au terme des délais de recours.

Afin de répondre au mieux à vos besoins et vous établir une proposition chiffrée,
vous pouvez me communiquer le protocole électoral par e-mail à vote-electronique [ar-obas-e]lenetexpert.fr ou à défaut, me communiquer quelques informations relatives à vos élections en remplissant un formulaire d'information accessible à partir du lien suivant :
https://www.lenetexpert.fr/questions-avant-expertise-solution-de-vote-par-voie-electronique

(1) Décret n°2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise
(2) Articles R2314-8 et R2324-4 du Code du travail
(3) Article R2324-6 du Code du travail
(4) Article R2324-7 du Code du travail
(5) Article R2324-8 du Code du travail
(6) Article R2324-9 du Code du travail
(7) Articles R2314-12 et R2324-8 du Code du travail
(8) Articles R2314-14 et R2324-10 du Code du travail
(9) Articles R2314-19 et R2324-15 du Code du travail

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l’organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L’Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

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

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

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

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

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport

d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

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

Contactez-nous

Article original de Juritravail : Vote électronique : les 3 points à retenir !

Mise en conformité RGPD : Ça veut dire quoi ?

Mettre un établissement en conformité avec le RGPD n'est pas qu'un objectif à la mode dont on parle dans les dîners mondains. C'est aussi une démarche utile pour ses client, son entourage professionnel et personnel, utile pour sa société, utile pour LA société !

Imaginez qu'un jour des inconnus puissent connaître les problèmes médicaux que vous avez eu par le passé et ceux qui hantent votre vie actuellement ?
Imaginez qu'un jour, pour la nième, fois vous deviez bloquer votre actuelle carte bancaire et en commander une autre car votre compte bancaire s'est à nouveau fait pirater ?
Imaginez qu'un jour vous soyez obligé(e) de changer d'adresse e-mail privée car vous recevez chaque jour des centaines de spams (emails non désirés) ?
Imaginez qu'un jour vous découvrez que vos identifiants et mots de passe se retrouvent en clair sur Internet ?
Imaginez qu'un jour vous receviez sans cesse des sollicitations publicitaires sur le téléphone perso dont seuls vos amis et quelques professionnels essentiels ont le numéro ?
Imaginez qu'un jour on puisse découvrir au grand jour vos listes de courses, vos déplacements, vos choix politiques, votre religion, vos empreintes digitales, la liste de vos éventuelles condamnations…
Face à l'explosion du nombre de cas de piratages informatiques ces dernières années, les cas de vols de données devraient eux aussi considérablement augmenter.

VOUS TROUVERIEZ ÇA NORMAL ?
Si vous avez répondu OUI, c'est que certainement vous n'avez pas vécu ces situations.
Si vous avez répondu NON, **vous comprenez alors l'intérêt d'obliger les professionnels à protéger vos données personnelles.**
14 MILLIONS DE FRANÇAIS VICTIMES DE HACKERS EN 2016
57% DES ENTREPRISES VICTIMES D'UNE CYBERATTAQUE EN 2016
SEULEMENT 102629 DOSSIERS DE MISE EN CONFORMITÉ AVEC LA CNIL REÇUS EN 2016 (sur 4,4 millions d'entreprises)
Vous commencez à comprendre l'intérêt d'obliger les professionnels à protéger les données qu'ils détiennent ?
Depuis 1978 une loi, la Loi Informatique et Libertés, oblige tout professionnel, association et administration qui détient des données personnelles (données appartenant à des personnes permettant de les identifier à l'échelle de la population nationale). Presque 40 ans plus tard, le résultat est catastrophique. Seulement, ces 2 dernières années, les millions de victimes de a cybercriminalité s'enchaînent à un rythme effréné sans que tous ces « fraudeurs » de la données personnelles, responsables de toute la nourriture numérique que l'on peut donner aux pirates informatique ne soient inquiétés.
C'est pour remettre tous ces organismes sur le droit chemin que les membres de la communauté Européenne on souhaité s'unir pour établir un règlement qui entrera en vigueur le 25 mai 2018. Ces règles Européennes consisteront à définir le cadre juridique selon lesquelles tous les organismes concerné seront tenus de protéger les toutes les données que nous leur avons communiquées en toute confiance.
A quoi ça sert de restreindre l'accès aux informations et aux photos du compte de votre réseau social préféré si par ailleurs, tous les dépositaires de vos données personnelles n'appliquent pas les mêmes précautions que vous !

CHERS PROFESSIONNELS
Le Règlement Général sur la Protection de Données (RGPD) entre en application le 25 mai 2018 et les entreprises ne s'y sont pas préparées. Or, elles sont toutes concernées, de l'indépendant aux plus grosses entreprises, et risqueront, en cas de manquement, des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires et des conséquences sur leur réputation. Un point indispensable sur cette mise en conformité obligatoire.
Au delà des amendes pouvant attendre plusieurs millions d'euros, c'est maintenant la réputation des entreprises qui est en jeu. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Les étapes d'une mise en conformité :
1. Établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique ;
2. Vérifier les spécificités et dispenses propres à l'activité ou au statut de l'établissement ;
3. Analyser chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement ;
4. Tenir un registre dans lequel seront référencés les différents traitements des données à caractère personnel conformes et à modifier ;
5. Tenir compte de l'évolution de l'entreprise et s'assurer que la conformité est maintenue.

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

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

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

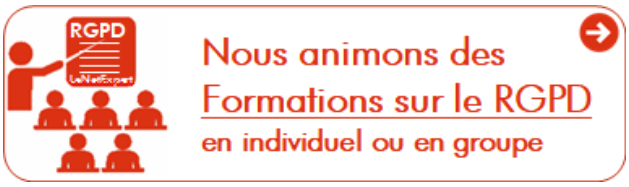
Contactez-nous

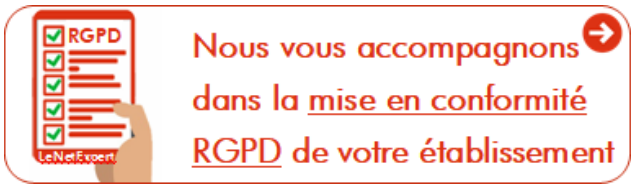
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Article de Denis JACOPINI

Utiliser un Wifi public ? Voici 5 précautions à prendre

Le plus souvent proposés gratuitement ou en échange de la collecte de données de navigation, certaines de ces connexions « gratuites » n'offrent pas les garanties suffisantes pour une navigation sécurisée.

Ces conseils valent aussi bien pour votre ordinateur (personnel ou professionnel) que pour votre smartphone ou votre tablette.

1.

Évitez de vous connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance

Plutôt que de vous fier uniquement au nom du réseau qui s'affiche, demandez systématiquement le nom du réseau au commerçant.En effet, il est très facile pour un pirate de créer un point d'accès WiFi au nom d'un restaurant puis de détourner l'ensemble du trafic qui y transitera. Cela peut par exemple permettre au pirate de récupérer les données que vous échangez avec un site de e-commerce ou encore d'obtenir vos données bancaires, les identifiants d'accès à votre compte, …

2.

Ne confiez pas trop d'informations à un portail d'accès Wi-Fi

Difficile de savoir si un portail d'accès Wi-Fi offre un niveau de sécurité satisfaisant ! Si celui-ci vous demande des informations personnelles en échange d'un accès à internet, évitez d'utiliser votre adresse mail principale, remplissez le moins d'informations possibles, et ne cochez pas la case « communiquer mes données à des tiers » à moins que vous ne souhaitiez que vos données soient transmises à des tiers afin qu'ils vous adressent des mails de prospection commerciale.

3.

Evitez de passer par un Wi-Fi public pour transmettre des données personnelles

Préférez passer par le réseau 3G/4G de votre opérateur internet. Si vous n'avez pas le choix, privilégiez toujours la visite de sites HTTPS et utilisez un VPN, de préférence payant ou que vous avez installé vous-même chez vous sur votre connexion personnelle.

4.

Désactivez la fonction Wi-Fi de votre appareil lorsqu'il n'est pas utilisé

N'activez pas la connexion automatique pour les réseaux WiFi autres que ceux de votre bureau ou votre domicile. Ainsi si vous repassez dans la zone de couverture du réseau, votre téléphone ne s'y connectera pas sans votre permission. Attention, même avec la fonction wifi désactivée, certains types de téléphones continuent d'émettre un signal Wi-Fi et sont susceptibles de permettre à des tiers de suivre vos déplacements, dans des centres commerciaux par exemple. Pour éviter cela, désactivez l'option « recherche toujours disponible » si votre téléphone vous le permet.

5.

et soyez à jour !

L'utilisation sécurisée d'un smartphone ou d'un ordinateur nécessite de maintenir le système d'exploitation et les pilotes Wi-Fi du terminal en permanence à jour des correctifs de sécurité. Appliquez régulièrement les mises à jour de sécurité proposées par le fabricant de votre smartphone, ou par l'éditeur de votre système d'exploitation.

LE SAVIEZ-VOUS ?

Les organismes (restaurant, aéroports…) qui proposent un accès au réseau internet au public, à titre payant ou gratuit, sont tenus de conserver les données de trafic de leurs clients. Ils doivent conserver les données techniques (ex. adresse IP, date, heure, durée de chaque connexion, informations permettant d'identifier le destinataire d'une communication). Les informations relatives au contenu des communications, comme l'objet ou le corps d'un courrier électronique ou bien les URL consultées sur un site web, ne doivent pas être conservées. Pour aller plus loin, consultez cette fiche.

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Utiliser un Wifi public ? Voici 5 précautions à prendre … | CNIL*

Devis pour la mise en conformité avec le RGPD de votre établissement

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Vous souhaitez faire appel à un expert informatique qui vous accompagne dans la mise en conformité avec le RGPD de votre établissement ?

Je me présente : Denis JACOPINI. Je suis Expert en informatique assermenté et **spécialisé en RGPD (protection des Données à Caractère Personnel) et en cybercriminalité**. Consultant depuis 1996 et formateur depuis 1998, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD20.

« Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. »

Pour cela, j'ai créé des services sur mesure :

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

• « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
• « Faire » (nous vous apprenons et vous poursuivez le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos cotés si vous en exprimez le besoin) ;
• ou « Nous laisser faire » (nous réalisons les démarches de mise en conformité de votre établissement en totale autonomie et vous établissons régulièrement un rapport des actions réalisées opposable à un contrôle de la CNIL).

contactez-nous avec le formulaire ci-dessous

Pour ceux qui veulent apprendre à faire, nous proposons 3 niveaux de formation

1. Une formation d'une journée pour vous sensibiliser au RGPD : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** » ;
2. Une formation de deux jours pour les futurs ou actuels DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** » ;
3. Une formation sur 4 jours pour les structures qui veulent apprendre à mettre en conformité leurs clients : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

Cliquez ici pour accéder à notre formulaire de demande d'informations

Source : Denis JACOPINI

L’ABC des bonnes pratiques pour se protéger des Cyberattaques | Denis JACOPINI

Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe
Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, $, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés
Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests
Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle
Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité
Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement
Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

Source : https://www.lesaffaires.com/classements/les-500/cyberattaques-l-abc-des-bonnes-pratiques/579150

LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr

Parce que les victimes doivent pouvoir compter sur des professionnels habitués à réagir face à des actes de piratage, des escroqueries ou vols de données etc., nous avons tenu à soutenir le projet cybermalveillance.gouv.fr. à mettant à leur disposition le meilleur de nos compétences.

2017 sera probablement l'année qui comptera le plus de victimes de rançongiciels. Les initiatives que l'on peut identifier sur le cyberespace ayant pour objectif de combattre ce fléau démontrent une réelle prise de conscience à toutes les strates de l'économie et de l'état. Vous trouverez ci-dessous un guide pdf spécialement fait pour vous aider à anticiper et à réagir face de telles menaces. Cette fiche réflexe est destinée à toutes les catégories de publics. Elle présente cette catégorie d'attaque informatique, les principales mesures à prendre pour s'en protéger, les actions à entreprendre lorsque l'on en est victime, ainsi que les infractions et sanctions pénales auxquelles s'exposent ceux qui les utilisent.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Réagissez à cet article

Source : *Fiche rançongiciels (cryptolocker)*

A quoi s'applique la loi « Informatique et Libertés ? | Denis JACOPINI

REMARQUE :
Le contenu de cette page date d'avant l'entrée en viguruer du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 appelé aussi RGPD (Règlement Général sur la Protection des Données). au 19/07/2020, la loi Informatique & Libertés est toutefois toujours en vigueur et a été modifiée depuis le 25/05/2018. Le contenu de ce document reste toutefois valable.

La loi « Informatique et Libertés » s'applique :

• Aux fichiers, systèmes, dispositifs informatisés ou non ;
• Comportant des informations concernant des personnes physiques (nom, adresse, photos, identifiants divers, etc.) ;
• Mis en oeuvre par une personne physique ou morale installée en France ou exerçant une activité professionnelle ou associative en France.

La loi « Informatique et Libertés » ne s'applique pas :
• Aux fichiers ne comportant que des informations sur des personnes morales (sociétés, associations, établissement public), sans mention de leurs dirigeants ou actionnaires, personnes physiques ;
• Aux fichiers créés par des particuliers pour leur usage privé (répertoire personnel, etc.).

S o u r c e :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=6C2979337DD5240A1A085F73F327AD22?name=La+loi+%22Informatique+et+Libert%C3%A9s%22%2C+elle+s%27applique+%C3%A0+quoi+%3F&id=491