

Compte Facebook piraté : Quelles sont les bons réflexes à avoir ? | Denis JACOPINI

21



Il arrive parfois de se faire pirater son compte Facebook. Soit parce qu'on a oublié de se déconnecter du site sur un ordinateur public, soit parce qu'on s'est fait voler d'une manière ou d'une autre son mot de passe. Il arrive aussi que des personnes se fassent passer pour vous et ouvrent un profil à votre nom avec vos informations et photos personnelles.

Dans ces cas de piratage ou d'usurpation d'identité, il importe de réagir rapidement pour empêcher toute possibilité de nuisance.
Première chose à faire : signaler le compte piraté ou usurpé à Facebook.

Si votre compte a été piraté

Signaler un compte piraté

Si vous pensez que votre compte a été piraté ou infecté par un virus, cliquez sur le bouton Mon compte a été piraté ci-dessous. Nous vous aiderons à vous reconnecter afin d'en reprendre le contrôle.

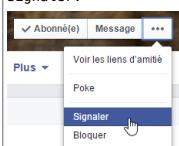
Annuler

Rendez-vous sur la page Signaler un compte piraté.

Indiquez l'identifiant de votre compte puis suivez les instructions. Vous serez notamment amené à taper votre ancien mot de passe et Facebook vous posera quelques questions pour vérifier votre identité.
Dans le pire des cas, vous pourrez faire appel à contacts de confiance pour récupérer votre compte.

Si votre identité (ou celle d'une autre personne) a été usurpée

Rendez-vous sur la page du profil suspicieux et cliquez sur le bouton contenant 3 petits points, juste en dessous de la photo de couverture. Sélectionnez Signaler.



Dans la fenêtre qui s'affiche alors, sélectionnez l'option Signaler ce compte et cliquez sur Continuer.

Aidez-nous à comprendre ce qui se passe

Que voulez-vous faire ?

Signaler du contenu partagé par Gauthier
 Signaler ce compte
 Obtenir de l'aide pour un autre problème

Dans l'écran suivant, sélectionnez ensuite l'option Ce journal se fait passer pour quelqu'un que je connais.

Aidez-nous à comprendre ce qui se passe

Quel est le problème avec ce compte ?

Cette personne me dérange
 Ce journal se fait passer pour moi ou quelqu'un que je connais
 Ce journal contient beaucoup de contenus inappropriés
 C'est un compte frauduleux
 Ce profil représente une entreprise ou une organisation
 Ce journal utilise un faux nom

Vous êtes amené ensuite à préciser votre cas.

Aidez-nous à comprendre ce qui se passe

Qui prétendent-ils être ?

Moi
 Une personne que je connais
 Une célébrité

S'il s'agit de votre propre identité, sélectionnez l'option Moi. Vous pouvez alors demander à fermer le compte.

Si l'identité de quelqu'un d'autre a été usurpée, sélectionnez l'option Une personne que je connais ou éventuellement Une célébrité.
Cliquez sur Continuer pour valider et suivez les instructions.

Aller plus loin et porter plainte

Si vous estimatez qu'il y a préjudice, vous pouvez aller porter plainte au Commissariat de police ou à la Gendarmerie de votre lieu d'habitation. N'hésitez pas à faire des captures d'écran pour nourrir votre dossier.

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.aussitot.fr/facebook/signaler-compte-pirate-usurpation-identite-facebook.html>

RGPD Règlement européen sur la protection des données : Une conformité basée sur la transparence et la responsabilisation



Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (*privacy by design*)

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

Les « études d'impact sur la vie privée » (EIVP ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Le Délégué à la Protection des données (Data Protection Officer)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

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

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

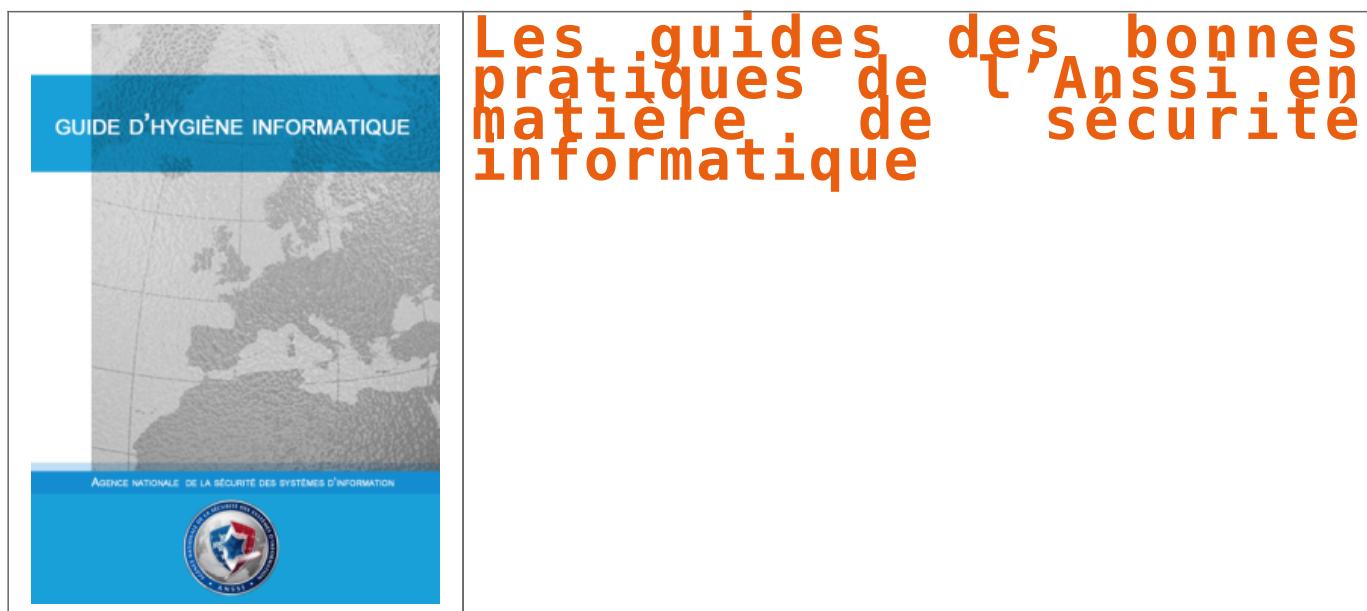


Contactez-nous

Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

Expert Informatique 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.ssi.gouv.fr/entreprise/bonnes-pratiques/>

RGPD Règlement européen sur la protection des données : Un renforcement des droits des personnes



**Règlement
européen sur la
protection des données
! Un renforcement des
droits des personnes**

Texte adopté par le règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transcription dans les différents Etats membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Deux tiers, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Le critère de « cléage »

Le règlement s'applique lors que la responsabilité de traitement ou le sous-traitant dont chaque pays de l'Union européenne ou que la responsabilité de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

La responsabilité des sous-traitants

Le règlement prévoit que la protection des données actuel concerne essentiellement les « responsables de traitements » et les modalités de traitement de données personnelles. Le règlement stan aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Le règlement prévoit que l'autorité de protection des données de l'Etat membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficiant ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transfrontaliers.

Une coopération renforcée entre autorités pour les traitements transfrontaliers

Le règlement prévoit que lorsque l'autorité « chef de file » n'a pas d'établissement dans l'Union, à savoir l'autorité de protection des données de l'Etat membre où se trouve leur « établissement principal », les autorités de protection des données des différents Etats concernés seront juridiquement compétentes pour assurer la conformité du traitement des données mis en œuvre.

Atte d'une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

En pratique, l'autorité « chef de file » proposera des mesures ou décisions (constituant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposeront alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis sera communiqué à l'autorité « chef de file » et à l'autorité « chef de file » portera la décision unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront enfin exécute, si elles sont défavorables, susceptible de recours devant le Conseil d'Etat.

Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront exécute, si elles sont défavorables, susceptible de recours devant le Conseil d'Etat.

Par ailleurs, certaines portent aussi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un blemment au règlement et garantir une sécurité suffisante aux entreprises et leur assurer une réponse unique sur l'ensemble du territoire de l'Union.

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 ?

A lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

Le RGPD (Règlement UE 2016/679) : tout ce qu'il faut savoir

Le RGPD, le règlement Européen de protection des données personnelles : RGPD ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre métier : Vous accompagnez 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 d'audit 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).

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

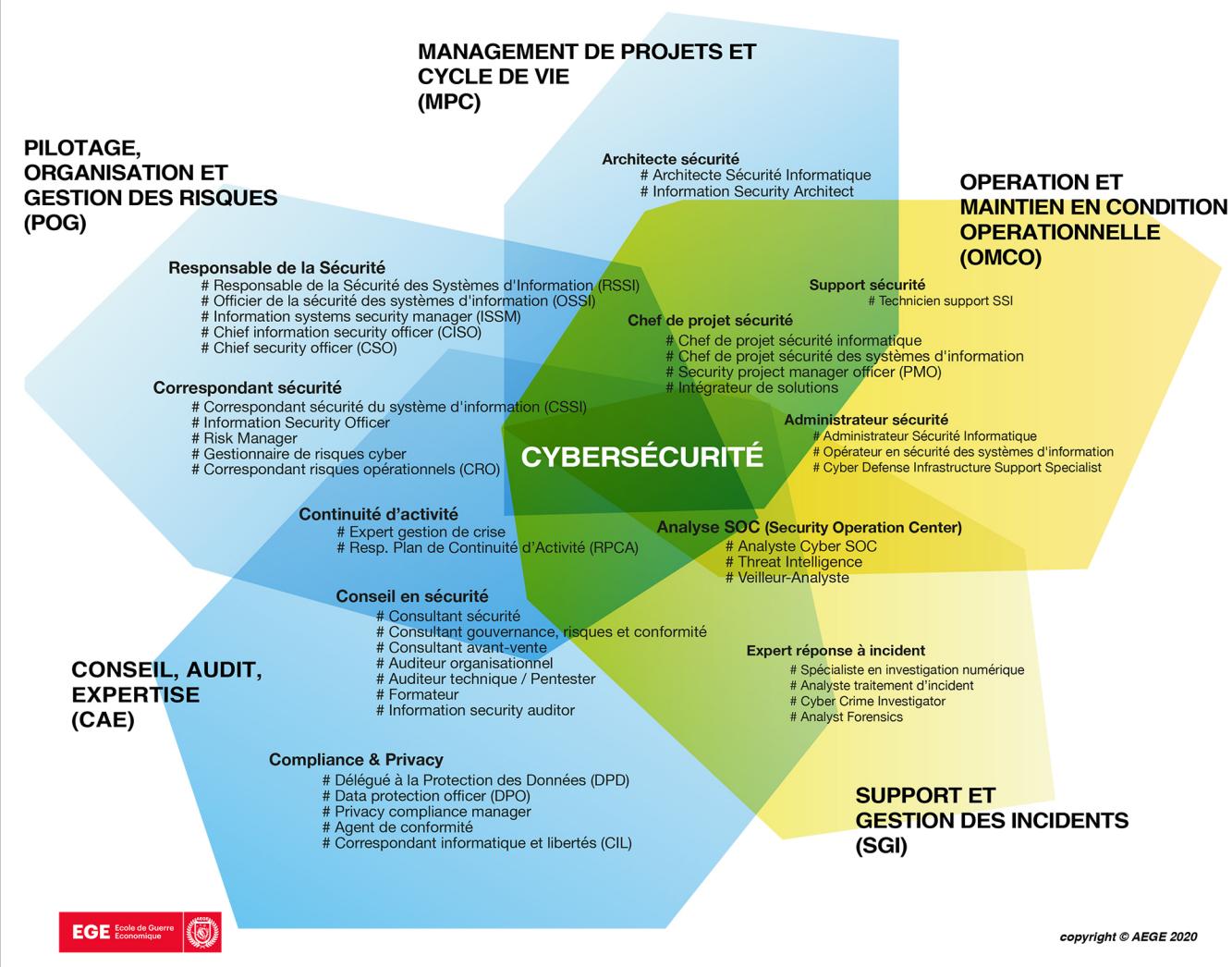


Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Les métiers de la cybersécurité en 2020

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
LE NET EXPERT AUDITS & EXPERTISES	EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LENETEXPERT .fr	LE NET EXPERT MISES EN CONFORMITÉ	SPY DETECTION Services de détection de logiciels espions	LE NET EXPERT FORMATIONS	LE NET EXPERT ARNAQUES & PIRATAGES
	Les métiers de la cybersécurité en 2020				
Denis JACOPINI vous informe					

L'Ecole de Guerre Economique et le Club Cyber de l'AEGE publient la « Cartographie des métiers de la Cybersécurité » dans le cadre des formations dispensées à l'Ecole depuis 2016. Les zones bleues se rapportent à des familles de métiers Cyber typés management, alors que celles en jaune sont plus orientés ingénierie et technique.



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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez

plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *L'Ecole de Guerre Economique publie la cartographie des métiers de la cybersécurité 2020 | Ecole de Guerre Economique*

Attention aux démarchages trompeurs « Mise en conformité RGPD »

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LE NET EXPERT .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
--	--	---	---	---	---



Denis JACOPINI
DENIS JACOPINI
EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ
vous informe

Attention aux démarchages trompeurs « Mise en conformité RGPD »

Des courriers « Mise en conformité – RELANCE » ou « Mise en conformité – dernier rappel » avec le logo usurpé de la CNIL ou des fax « RGPD – Mise en conformité » invitent à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen.



MISE EN CONFORMITE RELANCE

Nom du dossier :

Code contact :

Date : 19/09/2018

Objet : RGPD - Mise en conformité RGPD

Madame, Monsieur,

Nous vous rappelons qu'à compter du 25 mai 2018, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Vous êtes invités à vous mettre en conformité sans délai.

Le Pôle administratif RGPD a mis en place un service d'assistance téléphonique centralisé, intégralement dédié à cette circonstance, disponible du lundi au vendredi de 9h00 à 18h00 au :

- Par téléphone : (prix d'un appel local)

- En ligne : Remplir le questionnaire de pré diagnostic RGPD en ligne

Si vous avez déjà effectué votre rapport RGPD, merci de ne pas tenir compte de ce rappel.

Pôle Administratif RGPD

Le directeur régional



RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) - sanctions prévues

(Chapitre III, article 83, alinéa 1)

Les responsables de traitement peuvent être tenus responsables administratifs pouvant s'élever jusqu'à 20 000 000 EUR ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

(Chapitre III, article 83, alinéa 2)

Sanction maximale pour violation de l'obligation de notification ou de communication ou de conservation des données personnelles lorsque celles-ci sont sensibles ou lorsque celles-ci ont été volées ou fait l'objet d'un vol ou d'un vol intentionnel de ces données à caractère personnel effectué en violation du présent règlement.

(Modifié par la loi 2009-091 du 10 avril 2009)

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel auxquels il figure dans la liste des facteurs. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut l'être identifiée.

RGPD

D'après des témoignages récents, après avoir appelé au numéro indiqué sur leur document affichant fièrement une bande bleu / blanc / rouge, ils ont posé quelques questions sur l'entreprise puis envoyé par mail un facture proforma demandant de s'en acquitter sous 72h. Les escrocs vont même jusqu'à dire qu'en payant cette facture, la CNIL fera une « levée de contrôle et de sanction » sur votre société.

Puis, une fois le paiement effectué, vous aurez un entretien de 15 minutes durant lequel 50 questions vous seront posées puis sous 30 jours un « délégué syndical du département » prendra contact et clôturera définitivement la mise à jour.

Tous ces arguments sont strictement faux !

La mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par une personne qualifiée en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps. Il est nécessaire, avant tout engagement, de chercher en ligne des informations sur la société qui prend contact avec vous. Si le doute persiste, vous pouvez contacter la CNIL au 01 53 73 22 22.

Pour vous rassurer, Denis JACOPINI et son équipe réalisent des démarches de mise en conformité des établissements avec la réglementation relative aux données à caractère Personnel depuis 2012. Plus d'informations ici

Nos conseils

Mettre en conformité nécessitera dans la plupart des cas une analyse de vos process, une sensibilisation du personnel, des interviews personnalisées et nous recommandons a minima une rencontre. Ces organismes ne semblent pas répondre à ces recommandations.

Au regard de pratiques commerciales trompeuses, la DGCCRF et la CNIL formulent plusieurs recommandations qui visent à :

- vérifier l'identité des entreprises démarchueuses qui ne sont en aucun cas, contrairement à ce que certaines prétendent, mandatées par les pouvoirs publics pour proposer à titre onéreux des prestations de mise en conformité au RGPD ;
- vérifier la nature des services proposés :
 - la mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps ;
 - Dans certains cas, il peut aussi s'agir de manœuvres pour collecter des informations sur une société en vue d'une escroquerie ou d'une attaque informatique.

Principaux réflexes à avoir en cas de démarchage

Si vous recevez ce type de sollicitations, vous devez :

- demander des informations sur l'identité de l'entreprise démarchueuse permettant de faire des vérifications sur internet ou auprès des syndicats de votre profession ;
- demander le numéro SIRET de l'organisme ;
- demander les conditions générales de vente de l'organisme ou les termes du contrat que vous devrez signer ;
- consulter le site internet et vérifier les mentions légales ;
- vérifier l'ancienneté du nom de domaine (un nom de domaine récent indique la création récente du service avec un risque de manque d'expérience ou la création d'un nom de domaine spécialement pour l'arnaque).
- vous méfier de telles communications prenant les formes d'une information officielle émanant d'un service public ;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;
- prendre le temps de la réflexion et de l'analyse de l'offre ;
- diffuser ces conseils de vigilance auprès de vos services et des personnels qui sont appelés à traiter ce type de courrier dans l'entreprise ;
- ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse..

Pour vous aider dans votre mise en conformité au RGPD, la CNIL publie des contenus pratiques. Vous pouvez notamment consulter « RGPD : ce qui change pour les pros » ainsi que le nouveau « Guide de sensibilisation pour les petites et moyennes entreprises » élaboré en partenariat avec la BPI.

Pour information, voici les 6 phases recommandées par la CNIL

<https://www.cnil.fr/fr/principes-cles/rgrp-se-preparer-en-6-etapes>

et notre méthode de mise en conformité avec le RGPD :

- « Comment se mettre en conformité avec le RGPD ? »
- « Mise en conformité RGPD : Accompagnement personnalisé par un Expert »
- « Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants ».



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai 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, j'ai été ensuite Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur.

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

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Vigilance : Démarchages trompeurs « Mise en conformité RGPD » | CNIL*

Illustration issue d'un témoignage

Comment éviter de se faire avoir par des e-mails de phishing

Comment éviter se faire avoir par des e-mails de phishing



Phone security | Ervins Strauhmanis via Flickr CC License by

Toujours, toujours être sur ses gardes.

Ça n'arrive qu'aux autres, à ceux qui ne font pas attention, qui n'y connaissent rien, qui font n'importe quoi sur internet. Jusqu'au jour où ça nous arrive à nous. Ça, c'est se faire avoir par du phishing (du hameçonnage, en français), cette technique qui consiste à vous envoyer un e-mail en se faisant passer pour quelqu'un dans le seul but de vous faire cliquer sur un lien, et vous faire rentrer identifiants et mots de passe dans une nouvelle page vous les demandant.

À l'été 2014, on avait ainsi découvert que de nombreuses stars américaines s'étaient ainsi fait voler leur identifiant iCloud de cette façon, permettant aux pirates de collecter leurs photos privées, dont certaines ont ensuite fini par être partagées sur des forums. Même chose avec le piratage de l'adresse e-mail de John Podesta, l'ancien chef de campagne d'Hillary Clinton, lors de la dernière présidentielle américaine.

Le phishing marche, souligne ainsi Wired, qui explique que 100.000 nouvelles attaques ont lieu chaque jour, et que quelques milliers réussissent. En septembre 2016, une étude allemande montrait qu'un étudiant interrogé sur deux pouvait se faire avoir par le message d'un inconnu. Alors pour éviter de se faire avoir, le magazine américain propose trois solutions.

1. Tout d'abord, **toujours réfléchir avant de cliquer**. «Si quelque chose a l'air bizarre, c'est que ça l'est probablement», et «vous devriez toujours être réticents à l'idée de télécharger les pièces jointes et de cliquer sur les liens, peu importe s'ils ont l'air innocent, ou la personne qui les a envoyés». En clair, toujours regarder l'origine de l'e-mail, et si quelque chose semble louche, ne pensez même pas à télécharger ou cliquer sur quoi que ce soit.

2. Ensuite, **scruter la source**. L'étape basique mais qu'on oublie si souvent. Pour être sûr que ce e-mail provient bien de Google, Yahoo!, ou de votre banque, vous devriez vraiment vérifier l'adresse qui vient de vous l'envoyer. Cela veut dire regarder dans l'URL de l'adresse si rien n'a l'air louche, ou si des caractères n'ont pas été remplacés par d'autres pour vous tromper (sur cette image par exemple, l'émetteur a ajouté un deuxième «l» à «paypal»). Si l'adresse e-mail est bien la bonne, mais que le test semble bizarre, vérifiez que c'est bien la bonne personne qui vient de vous l'envoyer, en tentant de la joindre par un autre canal.

3. Enfin, **préparer ses arrières**. En clair, faites comme si vous alliez vous faire avoir un jour ou un autre, et assurez-vous de limiter déjà les dégâts. «Cela veut dire prendre des précautions de cybersécurité standards, comme mettre en place une authentification à plusieurs facteurs (on vous a fait un tuto ici), utiliser un gestionnaire de mots de passe ou un autre système pour créer des mots de passe unique et aléatoires, et sauvegardez vos données.» Parce qu'au fond, le vrai e-maillon faible dans toutes ces histoires se trouve entre la chaise et le clavier.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DGTIC n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Comment éviter de se faire avoir par des e-mails de phishing | Slate.fr*

**Votre responsabilité engagée
en cas de piratage de vos
données | Denis JACOPINI**



Votre responsabilité engagée en cas de piratage de vos données

Si vous venez faire pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-à-vis des données que ce support numérique renferme.

Imaginez que vous disposez de différents appareils numériques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un Malware (Méchanticiel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l' intention de nuire retenue. Par contre, en tant que professionnel, en plus d'être victime du piratage (l'intrusion cauée par une faille, un virus, un crypto virus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi godfrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous prendre une seconde claque vis à vis de la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amende vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret:

La société Cochamborgnals voit son système informatique piraté. Des investigations sont menées et le pirate informatico arrêté. Vis à vis de la loi Godfrain du 5 janvier 1988, le voleur risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochamborgnals n'était pas en règle avec la CNIL, la dénonce auprès de cette dernière.

Le responsable de traitement, généralement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.

Est-ce bien normal ?
Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boîtes e-mail.

Autre cas concret:

Monsieur Roudoulot-Mariotout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ? La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, réferez vous au cas contrôles précédent. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.

Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi Formateur en Protection des données personnelles (Autorisation de la Direction du Travail et de la Formation Professionnelle n°92 84 03001 84).
Nous pouvons vous animer des actions de sensibilisation ou de formation à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Plus d'informations sur : <https://www.teneteexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI


Denis JACOPINI est Expert Informatique et aussi Formateur en Protection des données personnelles (Autorisation de la Direction du Travail et de la Formation Professionnelle n°92 84 03001 84).
Spécialiste en cybersécurité et en protection des données personnelles, il a une expérience de 20 ans dans le secteur public et privé.
• Expertise technique (virus, espions,间谍软件, fraudes, piratages, ransomwares, logiciels malveillants, cryptomonnaies, ransomwares, logiciels malveillants, cryptomonnaies, etc.)
• Expertise de systèmes de vote électronique;
• Formation et conférences en cybersécurité ;
• Formation de l'Etat (Conseiller Informatique et Cybersécurité);
• Accompagnement à la mise en conformité RGPD.
Accompagnement à la mise en conformité RGPD.

Le Net Expert
INFORMATIQUE | CYBERCRIMINALITÉ

Réagissez à cet article
Original de l'article mis en page : [Informatique et Libertés : suis-je concerné ? | CNIL](#)

Les bons réflexes contre les attaques informatiques | Denis JACOPINI

Les bons réflexes contre les attaques informatiques

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale. Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une centaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évouer leurs revendications. On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonnage par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quant à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (c2c) pilotant des milliers de machines « zombies » permettant des attaques DDoS (Déni de service distribué). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malfactors utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

Expert Informatique 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

Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croître dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'un million d'e-mails*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi faillibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant. La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

Expert Informatique 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.journaldunet.com/solutions/expert/60082/attaques-informatiques-decryptage-du-phenomene-et-reflexes-a-adopter.shtml>

Par Sébastien Delcroix - NFrance