Attaques informatiques Comment s'en protéger ?



Attaques informatiques : Comment s'en protéger es cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.

fous les quinze jours en moyenne, une attaque sévère – où des données sont exfiltrées – est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les entreprises. Julien Robert, directeur de la sécurité chez SFR, résume les trois facteurs agissant sur la sécurité : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les fournisseurs d'expécés et l'encadrement d'un dats centre externe fortement conseillé.

Prévention

reventum.

All est difficile d'apir lorsque l'attaque a déjà en lieu », précise Sylvie Sanchis, chef de la Befti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

Les modes opératoire

L'importance de porter plainte

réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie », selon Ciryl Piat, Lieutenant-colonel de la gendarmerie nationale. Suite à une cyber-attaque, la plupart des treprises sont réticentes à porter plainte, par peur d'une anunsier réputation ou par scepticise vis-à-vis de la réelle utilité de cette procédure. Alice Cherif, chef de la section « cyber-rininalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments invantage de la company au charcite de la section à l'avantage d'identifier les éléments invantage d'identifier les éléments d'invantages que la plainte présente l'avantage d'identifier les éléments d'invantages que la plainte présente l'avantage d'identifier les éléments d'invantages que la plainte présente l'avantage d'identifier les éléments d'invantages que la plainte présente l'avantage d'identifier les éléments d'invantages que la plainte présente l'avantage d'identifier les éléments d'invantages de la réelle de la section « cyber-rininalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'invantages de la réelle de la section « cyber-rininalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'invantage d'identifier les

L'utilité du cloud

L'une des façons de sécurier ses données est de les confier à un tiers spécialiste qu'il les stockers en ligne sur un clause. «Il s'aguit du'il système complexe commencé sur Internet, où les données sont stockées sur des disques durs physiques située dans des salles d'hébergement, les fameur dars contrers », enplies deutre leurent, de les données. Vigilianes sont stockées sur des disques durs physiques située dans des salles d'hébergement, les fameur dars contrers », en les données. Vigilianes sont stockées sur des disques durs physiques située dans des salles d'hébergement, les fameur dars contrers », en les données. Vigilianes sont stockées sur des disques durs physiques située dans des salles d'hébergement, les fameur dars contrers », en les données vigilianes des salles d'hébergement, les fameur dars contrers », en les données vigilianes des salles d'hébergement, les fameur dars contrers de les confiers à un tiers sont des salles d'hébergement, les fameur dars contrers de les confiers à un tiers sont des salles d'hébergement, les fameur dars contrers de les confiers », en les confiers à un tiers sont des salles d'hébergement, les fameur dars contrers des des salles d'hébergement, les fameur dars contrers des des salles d'hébergement, les fameur dars contrers de les confiers à un tiers sont des salles d'hébergement, les fameur de la confiers de la confier de la c

(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



Original de l'article mis en page : Cybercriminalité : comment se protéger ? — Magazine Decideurs

LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr





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.





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

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



Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.

Les 3 axes vers lesquels votre structure devra progresser seront :

- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

[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 (Symantec) 13,8 Milions de victimes 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

Formation en cybercriminalité : Virus, arnaques et

piratages Solutions entreprises

informatiques, pour nos



Présentation

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos

comportements au quotidien.

Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des

attitudes responsables seront les clés permettant d'enrayer le phénomène....

Objectif

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer ce phénomène.

Durée

1 journée

ou conférence de 2 heures.

Public concerné

Chefs d'entreprise, présidents d'associations, élus, décideurs, employés, agents,

Moyens pédagogiques

Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

Animateur

Denis JACOPINI

Expert Judiciaire en Informatique diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire. Spécialisé en Protection des données personnelles et certifié ISO 27005, il a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Son métier : Aider les professionnels à <u>se protéger des pirates informatiques</u>, et à <u>se mettre en conformité</u> avec la CNIL et le règlement Européen sur la <u>Protection des Données Personnelles</u>.

Il intervient dans la France entière et à l'étranger pour former ou sensibiliser les décideurs, informaticiens et utilisateurs sur les techniques utilisées par les Pirates informatiques pour piéger leurs victimes et sur les obligations en matière de protection des données à caractère personnel.

Différentes interventions pour :

- Le Conseil de l'Europe ;
- Un Centre d'Enseignement et de Recherche en Informatique ;
- Le Centre d'Etudes des Techniques Financières et d'Ingénierie d'Aix en Provence ;
- Des écoles d'avocats ;
- Des Compagnies d'Experts Judiciaires ;
- De nombreux clubs ou associations de chefs d'entreprises dans la France entière et à l'étranger ;
- Le Centre National de la Fonction Publique Territoriale (CNFPT) pour des élus, des S.G. et des agents publics.

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle — Numéro formateur : 93 84 03041 84)

Plus d'informations sur

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles [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"]

16% des entreprises victimes des Ransomwares. Réagissez !



Les ransomwares visent de plus en plus les entreprises françaises. Ce phénomène n'est pas près de s'arrêter au regard du business model très lucratif et de l'impunité juridique dont bénéficient les hackers.

Force est de constater que les hacker un plus d'un coup d'avance.

En effet, PC Cyborg, le premier Ransomware, date tout de même de 1989. Pourtant, depuis le temps, le phénomène n'ayant pas été pris au sérieux, il commence désormais à prendre une ampleur phénoménale.

Il est évident qu'aujourd'hui aussi bien les entreprises que les états sont dépassés par ce phénomène. La liste des entreprises, parfois des OIV (Opérateurs d'importance Vitale) ou des OSE (Opérateur de Services Essentiels) ou des services publics touchés ne cesse de s'alourdir.

Que nous annonce le futur ?

Nos télévisions prises en otage par un ransomware (crypto virus ou programme informatique qui rend illisible vos données et inversera l'opération contre paiement d'une rançon, d'où le nom de crypto virus) pourrait bien arriver dans nos foyés dans les prochains mois. Notre auto, notre téléphone et bientôt nos maisons (serrures, lumières, fours, réfrigérateurs... n'importe quel objet connecté essentiel en définitive) pourraient bien nous demander un petit bitcoin en échange de son refonctionnement.

Que pouvons nous faire ?

Les entreprises doivent évoluer selon plusieurs axes :

- Reconsidérer la priorité consacrée à la sécurité informatique pour faire évoluer son infrastructure technique, organisationnelle, reconsidérer les conséquences en terme d'image ou de pérennité que pourraient entraîner une attaque informatique.
- Reconsidérer le personnel en charge du service informatique et former le responsable informatique à la sécurité ou mieux (ce que je recommande), utiliser les services d'un expert en cybersécurité ou en cybercriminalité en appui du service informatique.
- Responsabiliser les utilisateurs par une charte informatique complétée et présentée lors des cessions de sensibilisation.
- Sensibiliser (et former pour certains) les utilisateurs aux différents risques liés aux usages informatiques en partant des ransomwares, jusqu'aux différentes formes d'arnaques aux victimes dépouillées de plusieurs dizaines, centaines milliers d'euros voire des millions d'euros.

Et au niveau international ?

Il est évident que la tâche sera longue et fastidieuse mais il est à mon avis possible de combattre le phénomène en agissant sur plusieurs leviers.

Le voler législatif doit évoluer et s'adapter aux attaques informatiques internationales pour que les coopérations internationales puissent se passer sans délai.

Le volet coordination doit être couvert par une entité internationale qui pourrait devenir un point de contact aussi bien pour les autorités collectant les plaintes de victimes, pour les organismes faisant évoluer les instruments judiciaires, pour les éditeurs et constructeurs d'outils exposés au menaces.

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

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

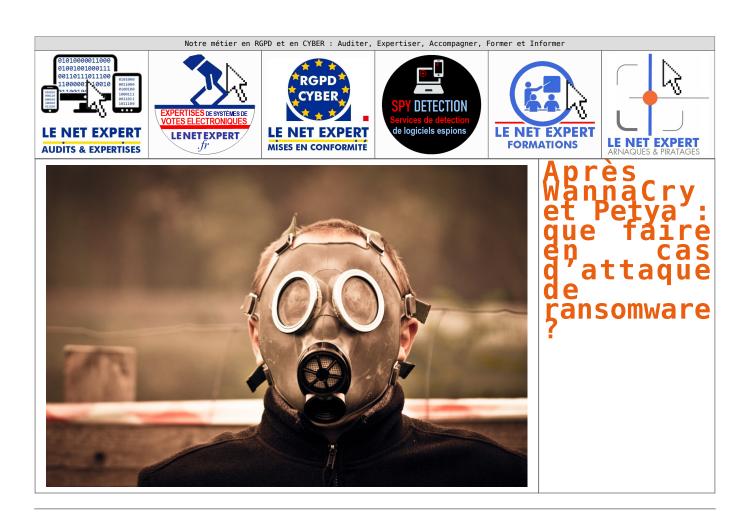
Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

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

Attaques informatiques : comment les repérer ?

Source : Denis JACOPINI

Après WannaCry et Petya : que faire en cas d'attaque de ransomware ?



Bruxelles, le 17 juillet 2017 — C'est le plus grand cauchemar des équipes de sécurité : une attaque de ransomware comme WannaCry ou Petya. Balabit, fournisseur leader de solutions de gestion des accès privilégiés (PAM) et des logs, a reçu pendant ces attaques des informations en temps réel de ses clients et d'autres professionnels de la sécurité. L'organisation a aidé d'autres entreprises à minimiser leurs risques, tandis que sa propre équipe de sécurité a analysé les risques encourus en interne. Grâce à cette expérience, Balabit a reconstitué le déroulement des attaques afin d'en tirer des leçons. Que doivent donc faire les organisations pour contrer les programmes malveillants ? Elles doivent prendre les cinq mesures suivantes.

Publié dans informaticien.be par zion

1. Isolez

Débranchez aussi vite que possible les appareils tels que les téléphones et les ordinateurs portables. Si vous êtes contaminé par un programme malveillant, retirez aussitôt le câble d'alimentation.

2. Collectez des informations

Qu'est-ce que c'est ? Quel est son mode opératoire ? Comment s'en prémunir ? Des équipes de désastre informatique nationales sont-elles disponibles ? Utilisez les plates-formes les plus pratiques pour diffuser ces informations : Twitter et les blogs de sécurité. Et bien sûr aussi la communication informelle entre entreprises.

3. Segmentez le réseau

Isolez le protocole infecté dans le trafic réseau. C'est une décision difficile : allez-vous contrer la diffusion du programme malveillant ou bien maintenir vos processus métier ?

4. Déployez des contre-mesures

Utilisez des Indicateur de compromission (IOC) et mettez à jour votre Système de détection des intrusions (IDS) et les paramètres du firewall, des systèmes AV et d'autant de serveurs et clients Windows que possible. Dans l'intervalle, les fournisseurs d'anti-virus travaillent évidemment sur une réponse adaptée à l'attaque.

5. Croisez les doigts et espérez

Anticipez l'avenir. Qu'est-ce qui se prépare ? Peut-être une nouvelle variante ? Tous les systèmes ont-ils eu leur patch ? L'organisation doit-elle craindre de figurer dans les journaux demain ? Une chose a-t-elle été perdue de vue dans l'urgence ? Étudiez tous les scénarios et essayez ainsi d'éviter un nouveau problème.

[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 : Après WannaCry et Petya : que faire en cas d'attaque de ransomware ? — Press Releases — Informaticien.be

Les 6 conseils pour se protéger des Cryptovirus (Ransomwares)



Alors que l'ANSSI vient d'annoncer un MOOC pour aider les entreprises à bien se protéger suite aux dernières attaques informatiques comme WannaCry, on réalise que la sécurité d'une entreprise doit être avant tout l'affaire de tous ses employés, et pas simplement des équipes dédiées au sein du service informatique. Après tout, la capacité de résistance de toute organisation dépend de son maillon le plus faible.

Une partie des financements devrait avoir pour objectif d'aider les entreprises à développer un programme de sensibilisation aux pratiques de cybersécurité spécialement adapté aux problématiques des PME. En effet, contrairement à leurs homologues des grandes entreprises, les dirigeants des PME sont généralement davantage impliqués dans des décisions d'ordres variés ce qui influe directement sur leur capacité à consacrer le temps ou l'attention nécessaires à la sécurité des systèmes d'information.

Tout programme conçu pour sensibiliser les employés aux méthodes de protection des menaces devrait en premier lieu viser à développer les connaissances des meilleures pratiques à tous les échelons hiérarchiques. Thibaut Behaghel, Spécialiste Produits International au sein du gestionnaire de mots de passe LastPass, nous explique à quoi pourrait ressembler un tel programme pour les petites et moyennes entreprises, et qu'elles devraient en être les priorités.

1.Respecter les principes de bases

En matière de sécurité, il existe un certain nombre de principes de base à suivre pour toutes les organisations, à commencer par la mise en place de règles concernant la longueur, la complexité et la durée de validité des mots de passe…[lire la suite]

2.Gérer les accès des utilisateurs

Quel que soit le nombre d'employés de votre entreprise, il est essentiel que chacun d'entre eux n'ait accès qu'aux informations et aux données qu'il est autorisé à consulter…[lire la suite]

3.Définir une politique de sécurité

Toute organisation devrait créer une politique détaillant les mesures de sécurité prises à la fois au niveau de l'entreprise elle-même, et par l'ensemble de ses employés...[lire la suite]

4. Former les salariés

Une fois la politique de sécurité mise en place, il est nécessaire de former les employés afin qu'ils en connaissent les règles et qu'ils sachent comment les respecter…[lire la suite]

5.Sécuriser les réseaux sans fil

Les PME doivent utiliser des mots de passe administrateurs et d'accès aux réseaux forts, et choisir des protocoles de chiffrement éprouvés (WPA2 et AES)...[lire la suite]

6.Savoir reconnaître le phishing

En cas de doute, il ne faut prendre aucun risque. Les entreprises doivent montrer à leurs employés comment repérer et signaler des e-mails suspects…[lire la suite]

[lire la suite]

[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 : Ransomware : les 6 conseils pour se protéger

Comment bien se protéger contre les Cyberattaques ?



Comment bien se protéger contre les Cyberattaques ?

On l'a encore vu récemment, aucun système informatique n'est à l'abri d'une faille...

Et en matière de cybercriminalité, les exemples nous montrent que l'attaque semble toujours avoir un coup d'avance sur la défense. L'enjeu, pour les institutions et les entreprises, est d'anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d'informations, cyberespionnage économique ou industriel…, en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n'est malheureusement pas à l'amélioration et

l'actualité récente regorge d'exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l'on connait, l'attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale…, les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes : 1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;

- 2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu'humaines ;
- 3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
- 4. Assurer une surveillance des mesures de sécurité et s'assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.
 - Vous souhaitez faire un point sur l'exposition de votre entreprise aux risques cyber ?
- Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu'il ne soit trop tard ?
- Vous rechercher une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

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 RGPD (Protection des Données à Caractère Personnel).



- Audits RGP
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e mails, contentieux, détournements de clientèle...;
- Expertises de systèmes de vote électronique



Contactez-nous



Réagissez à cet article

Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?



Conseils pour bien se protéger des demandes de rançon informatiques rancongiciels ransomwares cryptovirus Les rançongiciels (ransomware en anglais) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon pour en obtenir à nouveau l'accès.

Depuis 2013, une variante est apparue avec des virus chiffrants ou crypto-virus (cryptolocker, cryptoDefense, cryptorBit et plus récemment locky, petya ou WannaCry). Cette forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent parfois la clé de déchiffrement une fois le paiement de la rançon effectué, mais ce n'est jamais une garantie.

Cliquez ci-dessous pour en savoir plus:



Victime d'un rançongiciels / ransomwares / cryptovirus ou d'une demandes de rançon informatiques ? Contactez-nous

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 DRTEF 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 : Les rançongiciels ou ransomware — ANSSI — Plateforme Cyber Malveillance

Un outil gratuit pour analyser et nettoyer votre ordinateur



Un outil gratuit pour analyser et hettoyer votre ordinateur Avec plus de 40.000 visiteurs uniques par an, ESET Online Scanner apparaît comme l'un des outils gratuits les plus plébiscités par les internautes soucieux de leur sécurité. Fort de ce constat, ESET améliore son scanner basé sur le moteur d'analyse ThreatSense® permettant d'analyser et nettoyer son ordinateur sans contrainte d'installation logicielle.

Conçue pour être conviviale, cette dernière version devient complètement indépendante des navigateurs Internet. De plus, l'installation est désormais possible sans les droits d'administrateur, ce qui rend l'analyse et le nettoyage des ordinateurs contenant des logiciels malveillants encore plus simples.

ESET Online Scanner améliore l'élimination des logiciels malveillants, par l'ajout de ces nouvelles fonctions :

- Analyse des emplacements de démarrage automatique et du secteur d'amorçage pour les menaces cachées choix de cette option dans setup / cibles d'analyse avancées
- **Nettoyage du registre système** Supprime les traces des logiciels malveillants du registre système
- Nettoyage après analyse lors du redémarrage Si nécessaire, ESET Online Scanner est capable de repérer les malwares les plus persistants afin de les nettoyer après redémarrage Pour plus d'informations sur l'outil gratuit ESET Online Scanner, contactez-nous ou rendezvous sur http://www.eset.com/fr/home/products/online-scanner/

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

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

Plus d'informations sur

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Original de l'article mis en page : Boîte de réception (10) — denis.jacopini@gmail.com — Gmail