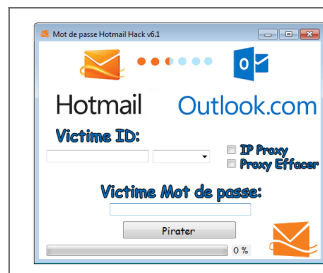


Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?



Quoi et comment
supprimer vos
données si vous
rendez votre
ordinateur
professionnel à
votre employeur ?



Votre boîte e-mail a été
piratée. Quelle attitude
adopter ?

Il vous semble ou vous avez la certitude que votre boîte e-mail a été piratée ? Quelle attitude adopter ?

Un choix s'offre à vous :

Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage

Il vous semble ou vous avez la certitude que votre boîte e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?

– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?

– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?

– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?

1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.

Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions... Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.

2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulièrement (e-mail, banque, blog, réseaux sociaux...).

Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte

Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.

Soit vous avez les éléments techniques pouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.

Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-sigalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachez que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis Jacopini anime des **conférences et des formations** 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.

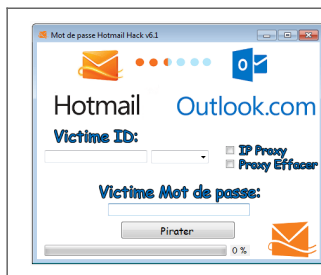
Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Arnaques, spams, phishing, sextape. Comment se protéger ? | Denis JACOPINI



Arnaques, spams, phishing,
sextape. Comment se protéger ?

Il vous semble ou vous avez la certitude que votre boîte e-mail a été piratée ? Quelle attitude adopter ?

Un choix s'offre à vous :

Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage

Il vous semble ou vous avez la certitude que votre boîte e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?

– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?

– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?

– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?

1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.

Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions... Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.

2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulièrement (e-mail, banque, blog, réseaux sociaux...).

Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte

Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.

Soit vous avez les éléments techniques prouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.

Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachant que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis JACOPINI est Expert Informatique assermenté, pratiquant à la demande de particuliers d'entreprises ou de Tribunaux. Il est consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.

Nos domaines de compétence :

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Déplacements professionnels. Attention au Wi-Fi de l'hôtel...



Déplacements
professionnels.
Attention au Wi-
Fi de l'hôtel...

Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) – Redirect

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres , informaticiens, responsable informatique, RSSI, utilisateurs).

[Contactez-nous](#)

PROGRAMME

CYBERCRIMINALITÉ **COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ**

Présentation

La France a rattrapé son retard en matière d'équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d'un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d'avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

Objectifs

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

[Demande d'informations](#)

CYBERCRIMINALITÉ

LES ARNAQUES INTERNET A CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Présentation

Que vous vous serviez d'Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

Objectifs

Découvrez les mécanismes astucieux utilisés par les arnaqueurs

d'Internet dans plus d'une vingtaine cas d'arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

Demande d'informations

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Présentation

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées.

Au delà de ces amendes pouvant attendre plusieurs millions d'euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d'entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Cette formation non seulement répondra la plupart des questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

Objectifs

Cette formation a pour objectif de vous apporter l'essentiel pour comprendre et démarrer votre mise en conformité avec le

RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

Informations complémentaires

[Demande d'informations](#)

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Présentation

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

Objectifs

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

[Demande d'informations](#)

CYBERSÉCURITÉ

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Présentation

Que vous ayez déjà été victime d'une cyber-attaque ou que vous souhaitiez l'anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

Objectifs

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d'un acte ciblé avec l'intention de vous nuire, découvrez les procédures à suivre.

[Demande d'informations](#)

CYBERSÉCURITÉ

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d'intrusion, apprenez à réaliser l'indispensable audit sécurité de votre système informatique afin d'appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

Objectifs

Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.

[Demande d'informations](#)

CYBERSÉCURITÉ

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

Objectifs

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

[Demande d'informations](#)

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale, Investigation numérique pénale, et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute la France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaîne d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :
<http://www.leNetExpert.fr/contact>



Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de

passe » (à condition que...) | Denis JACOPINI



Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essaient de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse...* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, **plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier**, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui verrouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien verrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

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](#)

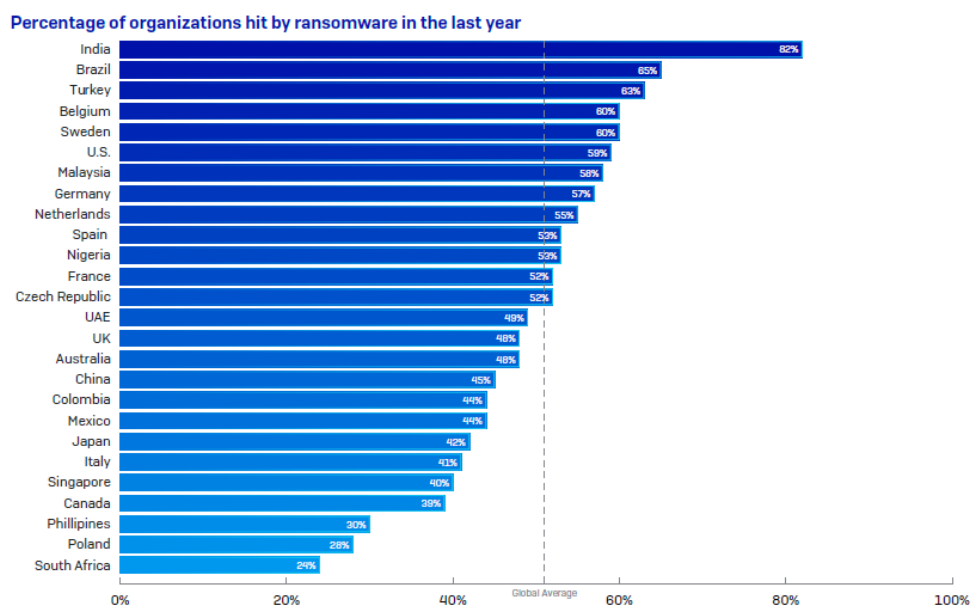
Réagissez à cet article

Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Atlantico.fr

52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe SPAM : GARE AUX ARNAQUES ! L'ESPION, DEVIENT ARNAQUEUR AU TRAVAIL. AUX DOSS. LES PRINCIPALES ARNAQUES DES RHES.		52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois			

En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.



LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE

« Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (...) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données », a expliqué Chester

Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

...[lire la suite]

Commentaire de notre Expert : Denis JACOPINI

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

Les conséquences

Il n'est plus à rappeler qu'être victime d'un ransomware entraînent un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malveillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

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 : *Etude : Payer la rançon multiplie par deux le coût total d'un ransomware*

« Vous avez été en contact avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones



	<p>« Vous avez été en contact avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones</p>
---	--

MÉFIEZ-VOUS ! – La crise sanitaire liée à la pandémie est perçue comme une opportunité par les pirates informatiques qui jouent sur les craintes et les angoisses des citoyens pour les piéger. Attention donc si vous recevez des messages liés au Covid-19 sur votre téléphone.

A l'approche de la levée du confinement, profitant de l'inquiétude qui règne au sein de la population, les pirates informatiques agissent, multipliant fraudes et arnaques sur le web, notamment à travers la pratique de l'hameçonnage (ou « phishing » en anglais), particulièrement lucrative. Pour rappel, cette technique consiste à « piéger » une personne en le poussant à cliquer sur un lien dans le but d'installer un logiciel malveillant sur son appareil ou de collecter ses informations personnelles. ...[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 : « Vous avez été en contact avec une personne testée positive au Covid-19 » : attention aux arnaques sur les smartphones | LCI

Le prestataire informatique responsable en cas de perte de données par un cryptovirus

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe		Le prestataire informatique responsable en cas de perte de données par un cryptovirus			

Un arrêt de la Cour d'Appel de Paris, dans un litige entre un prestataire de maintenance et son client, vient rappeler qu'un virus ou un ransomware ne constituent pas un cas de force majeure permettant d'exonérer qui que ce soit de ses obligations.

Le litige est né en 2016 mais la Cour d'Appel de Paris vient de le juger après une décision de première instance du tribunal de commerce en janvier 2018. Si l'affaire est assez complexe et avec de nombreuses ramifications sur la responsabilité et les manquements de chaque partie, un point particulier mérite d'être relevé. En l'occurrence, un crypto-virus a rendu inexploitable les sauvegardes et les données de l'entreprise cliente, problème de plus en plus fréquent de nos jours. Le prestataire a voulu faire considérer ce fait comme une circonstance de force majeure l'exonérant de sa responsabilité. La Cour d'Appel vient rappeler qu'un virus n'est aucunement un cas de force majeure (Cour d'appel de Paris, Pôle 5 – chambre 11, 7 février 2020, affaire n° 18/03616, non-publié)...

Commentaire de notre Expert : Denis JACOPINI

Il est évident qu'à partir du moment où un prestataire informatique vend un service de sauvegarde et assure d'une quelconque manière sa maintenance, il devient responsable de la réalisation de cette prestation, quelles qu'en soient les conditions excepté dans des situations appelés cas de force majeure.

En droit, les conditions de la force majeure évoluent au gré de la jurisprudence et de la doctrine. Traditionnellement, l'événement doit être « imprévisible, irrésistible et extérieur » pour constituer un cas de force majeure. Cette conception classique est cependant remise en cause (Wikipédia).

Dans la vraie vie, la situation dans laquelle s'est produit la perte de données doit être vue d'un peu plus près. Il n'y a pas à mon avis un cas de figure mais des cas de figure et les situations doivent être étudiées au cas par cas (chers avocats, je suis à votre disposition).

Certes, il est vrai, que le cryptovirus puisse être considéré comme imprévisible et extérieur, mais l'article 1218 du Code Civil précise :

« Il y a force majeure en matière contractuelle lorsqu'un événement échappant au contrôle du débiteur, qui ne pouvait être raisonnablement prévu lors de la conclusion du contrat et dont les effets ne peuvent être évités par des mesures appropriées, empêche l'exécution de son obligation par le débiteur »

C'est là que la balance du mauvais côté pour le prestataire informatique. Depuis 1989, date du premier cryptovirus (PC Cyborg) et pour être un peu plus gentil, depuis 2017, année durant laquelle le nombre de cas de rançongiciels a explosé de plusieurs centaines de pourcents, les cryptovirus sont prévisibles et les effets peuvent être évités par des mesures appropriées.

Ainsi, mesdames et messieurs les prestataires informatiques, mesdames et messieurs les chefs d'entreprises, je ne peux que vous recommander de faire auditer techniquement et juridiquement vos services de sauvegarde afin d'en analyser les risques résiduels car seule une analyse de risques permettra non seulement d'avoir une visibilité technique complète de votre services, mais vous pourrez également adapter vos contrats au résultat de cette dernière et convenir avec vos clients de l'existence ou non de cas pour lesquels la panne de votre système de sauvegarde sera « éligible » au cas de force majeure.

Intéressé par la réalisation d'un tel audit ?

N'hésitez pas à me contacter.

Denis JACOPINI (Expert informatique près les tribunaux diplômé en Cybercriminalité, Gestion des risques et Investigation Numérique)

[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 : *Justice : Un virus n'est pas un cas de force majeure*
– *Le Monde Informatique*

Une faille informatique concernant un milliard d'appareils connectés en Wi-Fi découverte !





D'après les chercheurs à l'origine de cette découverte, la vulnérabilité se trouverait dans les puces Wi-Fi fabriquées par Cypress Semiconductor et Broadcom. Parmi les appareils touchés, nous retrouvons les iPhone, iPad, Mac, ou les enceintes Echo d'Amazon, la Kindle, les appareils Android, ou encore le Raspberry Pi 3. D'après la société Eset, la faille affecterait principalement les puces WLAN FullMAC de Cypress et Broadcom. Pour information, les chercheurs ont nommé cette faille Kr00k.

Les chercheurs de l'Eset précisent que : *"cette faille de sécurité est gigantesque puisqu'un hacker peut déchiffrer des données qui ont été transmises par un point d'accès Wi-Fi vulnérable, sur près d'un milliard d'appareils"*. En réalité, **Kr00k exploite une faiblesse** qui se produit lorsque les appareils sans fil se dissocient d'un point d'accès sans fil. Plutôt que de chiffrer les données avec une clé pré-définie et utilisée lors de la connexion, les appareils vulnérables **utilisent une clé composée de zéros**, ce qui rend le déchiffrement très facile...[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 : *Un milliard d'appareils connectés en Wi-Fi touchés par une faille*