

Céder au chantage finance et renforce l'infrastructure des attaques DDoS | Denis JACOPINI

| | | | | | |
|---|---|--|---|--|--|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p> |  <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p> |  <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|  <p>Denis JACOPINI vous informe</p> | <p>Crypter données nouveau métier ?</p> | | | | |

La cybercriminalité peut prendre plusieurs formes (attaques DDOS, arnaques, spam...), Les pirates peuvent avoir plusieurs motivations (idéologie, vengeance, argent...) mais la technique qui aura le mieux fonctionné en 2015 et qui devra encore battre des records en 2016, c'est l'attaque par cryptolockers.

Je prends la peine d'écrire cet article car ces formes d'attaques feront dans les prochains mois, toujours partie non seulement des techniques les plus simples pour les pirates (2 milliards d'e-mails sont envoyés dans le monde chaque seconde dont la très grande majorité par des serveurs piratés), des plus rentables (même si seulement 0,01% des personnes se font infectées, je vous laisse calculer ou imaginer le nombre colossal de victimes chaque jour), et des moins risqués (en raison des technologies d'anonymisation facilement accessibles).

Qu'est-ce que les crypto lockers

Ce sont des programmes malveillants qui peuvent se cacher dans des pièces jointes de mails ou qui peuvent s'attraper en consultant des pages WEB infectées (des mails peuvent aussi transporter des pages WEB).

A l'ouverture des informations piégées, ces programmes malveillants se lancent automatiquement et commencent à crypter (coder les informations dans un code incompréhensible par l'humain), avec un code qui peut parfois être inconnu par les pirates eux-mêmes, la totalité des informations de vos disques durs (internes, amovibles, externes, réseaux...) et vous affichent, vers la fin de son travail, un message vous demandant de passer à la caisse.

Un règlement en bitcoins (monnaie virtuelle et anonyme de rigueur) vous sera demandé en échange du code permettant de décrypter vos données.

Si vous ne payez pas, vous êtes sûr que vos données ne seront pas décryptées; si vous payez, vous avez peut-être une chance de recevoir en échange de votre obole (quelques centaines d'euros) le code permettant de retrouver vos données comme avant.

Ces logiciels sont aussi appelés des rançongiciels ou des ransomwares (logiciel à rançon en français)

Comment s'en protéger

- Avoir des sauvegardes dignes de ce nom (automatisées, externalisées, historisées, contrôlées...) au cas où vous vous faites infecter ;
 - Avoir une suite de sécurité capable de bloquer les logiciels malveillants, les mails infectés ou les sites malveillants ;
- Redoubler de vigilance, surtout sur les sites proposant gratuitement des choses payantes (multimédia mais aussi pornographique).

Une solution que nous recommandons depuis plusieurs années :

Et si c'est trop tard

- Profiter enfin des sauvegardes que vous avez réalisées contraint et forcé sans vraiment croire qu'un jour vous en aurez besoin ;
 - Vous tourner vers un professionnel ou un service ayant l'outil de décryptage de vos données
 - Payer en espérant :
 - 1 : que vos données seront bien décryptées après paiement de la rançon;
 - 2 : qu'un seul logiciel malveillant ait crypté vos données (et qu'il n'y ait pas un logiciel qui vous a crypté des données déjà cryptées)
 - 3 : qu'aucun autre logiciel malveillant viendra vous refaire la même chose dans quelques jours car même si vous payez, rien ne vous garantit que, sans avoir activé des protections efficaces, vous ne vous refassiez pas infecter.
- [block id="24761" title="Pied de page HAUT"]

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



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

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

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

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

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3KI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité 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 CB avec Valérie BENHAÏM et ses invités.
Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UU0Hqj_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

La cybersécurité pour les débutants – Un lexique informatique

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

| | | | | | |
|--|---|--|--|---|---|
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i></p> |  <p>LE NET EXPERT MISES EN CONFORMITE</p> |  <p>SPY DETECTION Services de détection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|  <p>Denis JACOPINI vous informe LECI</p> | <p>La cybersécurité pour les débutants – Un lexique informatique</p> | | | | |

1. Introduction
2. Background
3. Methodology
4. Results
5. Discussion
6. Conclusion
7. References
8. Appendix
9. Glossary
10. Index

The following text is a placeholder for the main content of the document, which is currently blank.

[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"]

Original de l'article mis en page : Lexique – La préfecture de Police

Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une faute grave | Denis JACOPINI

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





Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une **#faute grave**

La cour d'appel de Lyon a confirmé le mois dernier le licenciement d'une salariée accusée d'avoir tenu sur Facebook des propos dégradants et injurieux à l'égard de ses collègues de travail. L'employeur n'a pourtant pas réussi à prouver que la personne mise en cause était bien l'auteur des messages délivrés sur un groupe spécialement créé à cet effet. Explications.

Travaillant en tant que sellière maroquinière depuis 2002 chez Hermès, Madame X est licenciée en décembre 2011 pour faute grave. C'est-à-dire sans préavis ni aucune indemnité. Il faut dire que les reproches formulés par son employeur sont relativement sérieux.

La salariée est en effet accusée d'avoir ouvert en octobre 2011 un groupe Facebook intitulé « Les potins d'Hermès », sur lequel étaient relatées des « situations tenant à la vie privée de certains collaborateurs nommément désignés », « sous forme de messages et anecdotes ». C'est suite à des remontées internes que la direction a eu vent de ces commentaires jugés « profondément dégradants et injurieux » à l'égard des employés concernés, ce qui a poussé les responsables de l'entreprise à chercher à remonter jusqu'à leur auteur.

Problème : l'administrateur de ce groupe dispose d'un compte Facebook au nom de « Jules César ». Autrement dit, il s'agit d'un beau pseudonyme... Après enquête, l'employeur affirme que l'adresse IP de l'auteur de ces messages correspond à celle du domicile de Madame X. Dans un premier temps, la salariée reconnaît avoir eu connaissance de ce groupe, tout en niant en être à l'origine. Mais dans un second temps, elle finit par admettre que le compte « Jules César » et le groupe « Les potins d'Hermès » ont bien été créés depuis son ordinateur, mais par sa sœur...

« Même dans le cas où les déclarations de votre soeur (par ailleurs très limitées quant à son hypothétique implication personnelle) [seraient] avérées, et dans la mesure où vous nous avez déclaré avoir eu connaissance de la création de la page et de son contenu dès sa mise en ligne, vous auriez dû à tout le moins nous alerter au sujet d'une telle initiative dont la teneur et la portée ne pouvaient rester sans conséquence vis-à-vis de l'entreprise et de ses collaborateurs » retient ainsi l'employeur dans sa lettre de licenciement.

Impossible d'identifier le créateur du groupe

Sauf que l'ex-salariée estime avoir été remerciée à tort. Elle a donc tout d'abord saisi le conseil des prud'hommes de Lyon, lequel a confirmé le licenciement pour faute grave en novembre 2013. Madame X a ensuite saisi la cour d'appel de Lyon, qui a justement rendu sa décision le 20 octobre dernier.

Les magistrats se sont intéressés en particulier aux adresses IP fournies par Hermès. Ils ont cependant constaté que la connexion ayant servi à créer le profil Jules César et à alimenter « la plupart » des messages litigieux correspondait en fait à « une adresse IP algérienne dont l'employeur n'a pu identifier le titulaire ». En clair, il était impossible de prouver en l'état qu'il s'agissait de Madame X ou même de sa sœur.

Mais cela n'a pas empêché la cour d'appel de considérer qu'il y avait malgré tout eu faute grave de la part de la salariée. Cette faute ? Savoir que le groupe « Les potins d'Hermès » existait et n'avoir rien signalé. La décision, que nous avons pu consulter, retient en ce sens que « la faute commise par Mme X en n'alertant pas sa direction sur la création de ce groupe de discussion alors qu'à partir de son propre ordinateur étaient mis en ligne des propos déshonorants pour ses collègues de travail (...) est d'une gravité suffisante pour rendre impossible le maintien de cette salariée dans l'entreprise pendant la durée limitée du préavis ».

La cour d'appel n'a donc pas donné suite aux demandes de l'ex-salariée, qui réclamait plus de 40 000 euros d'indemnités.

La décision de la cour d'appel de Lyon évoquée dans l'article ci-dessus

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source : <http://www.nextinpact.com/news/91031-propos-injurieux-sur-face-book-ne-pas-avertir-son-employeur-peut-etre-faute-grave.htm>

Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

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

| | | | | | |
|--|--|--|--|---|---|
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p> |  <p>LE NET EXPERT MISES EN CONFORMITE</p> |  <p>SPY DETECTION Services de detection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|--|--|--|--|---|---|



Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

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

2 SOLUTIONS POUR SE METTRE EN CONFORMITÉ AVEC LE RGPD

Vous apprenez à vous mettre en conformité avec le RGPD en suivant une formation (ci-dessous) ;

Vous faites appel à un expert / formateur qui vous accompagne dans votre mise en conformité avec le RGPD de votre établissement (Consultez notre page « Services d'accompagnement à la mise en conformité avec le RGPD »).



Je me présente : Denis JACOPINI. Je suis Expert de Justice en informatique spécialisée en cybersécurité 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, 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, il est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Pour cela, j'ai créé 3 niveaux de formation.

1. Une formation d'une journée pour les indépendants, TPE et les PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer ». Cette formation a pour objectif de vous faire découvrir l'essentiel de ce règlement Européen, de vous apprendre les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions ;
2. Une formation de deux jours pour les DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement ». Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement ;
3. Une formation sur 4 jours pour les consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD ». Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation est composée de 2 jours de théorie et 2 jours de pratique dont 1 dans l'établissement de votre choix (le votre ou celui d'un client). Suivez la formation qui vous apportera la plus grande autonomie avec le RGPD de tout notre catalogue.

et des services sur mesure.

1. Vous souhaitez tout faire -> Nous vous apprendrons à mettre votre établissement en conformité, la plupart du temps, le contenu de ces formations est personnalisé et adapté à vos besoins spécifiques ;
 2. Vous ne savez pas par où commencer -> Nous ferons l'état des lieux, mettrons en place le registre puis nous vous apprendrons à maintenir la conformité des traitements ;
 3. Vous ne souhaitez rien faire -> Nous nous occuperons de tout.
- Plus d'information sur nos services d'accompagnement à la mise en conformité avec le RGPD ici

Formation pour TPE/PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » : 1 jour

Découvrez l'essentiel du RGPD, apprenez les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions. Consultez les dates de nos prochaines formations

« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement. Consultez les dates de nos prochaines formations

« Je veux devenir le Délégué à la Protection des Données de mon établissement »

Formation pour consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour dans votre établissement

Enfin, si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez la formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue. Consultez les dates de nos prochaines formations

« J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Formation RGPD « Mise en conformité RGPD sur mesure » (pour TPE/PME)

(Pour ceux qui souhaitent une formation ou un accompagnement personnalisé dans la mise en conformité RGPD)

Que vous soyez bientôt ou déjà désigné « Délégué à la Protection des Données » ou « DPO » dans votre établissement, si vous souhaitez que nous établissions une formation personnalisée dans son contenu ou dans son organisation, nous nous ferons un plaisir d'étudier votre demande et d'élaborer une proposition adaptée à vos besoins.

Accompagnement à la mise en conformité RGPD de mon établissement

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

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

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

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » ;
- ou « Nous laisser faire ».

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

N'hésitez pas à contacter notre équipe.

Intéressé pour assister à une de nos sessions de formation en France, choisissez la ville qui vous intéresse. Vous souhaitez que nous nous déplaçons au sein de votre établissement pour une formation ou pour un accompagnement individuel, indiquez le dans les commentaires.

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

- la formation « Comprendre le RGPD » : 1 jour
- la formation « Je veux devenir Délégué à la Protection des Données » : 2 jours
- la formation « Je mets en conformité mon établissement » : 3+1 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs places à la formation :

Formation pour TPE/PME : « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : « Je veux devenir le Délégué à la Protection des Données de mon établissement »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre accepté. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre accepté sera remboursé en intégralité dans les 5 jours (Les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'accepté pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

LE FORMATEUR : Denis JACOPINI



Denis JACOPINI est Expert de Justice en informatique spécialisée en cybersécurité et en RGPD (protection des données à caractère Personnel). Il est diplômé en Cybersécurité, et, titulaire de l'expertise Judiciaire et est Certifié en Gestion des Risques des Systèmes d'Information. Il est formateur depuis 1998 et consultant depuis 1996, il a 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 dans la sécurité informatique, 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, il est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD à tout public.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

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



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

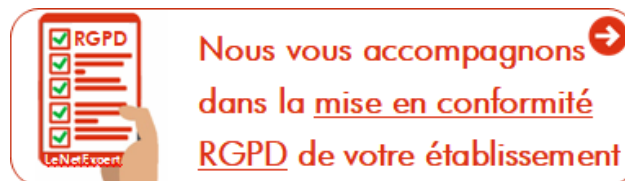
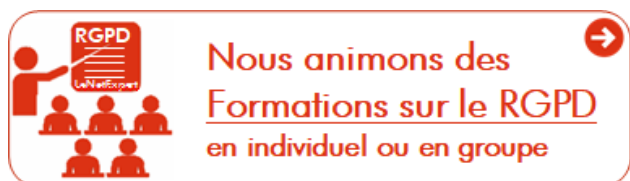
Contactez-nous

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

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

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

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



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles

en 6 étapes

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

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

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

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



Denis JACOPINI



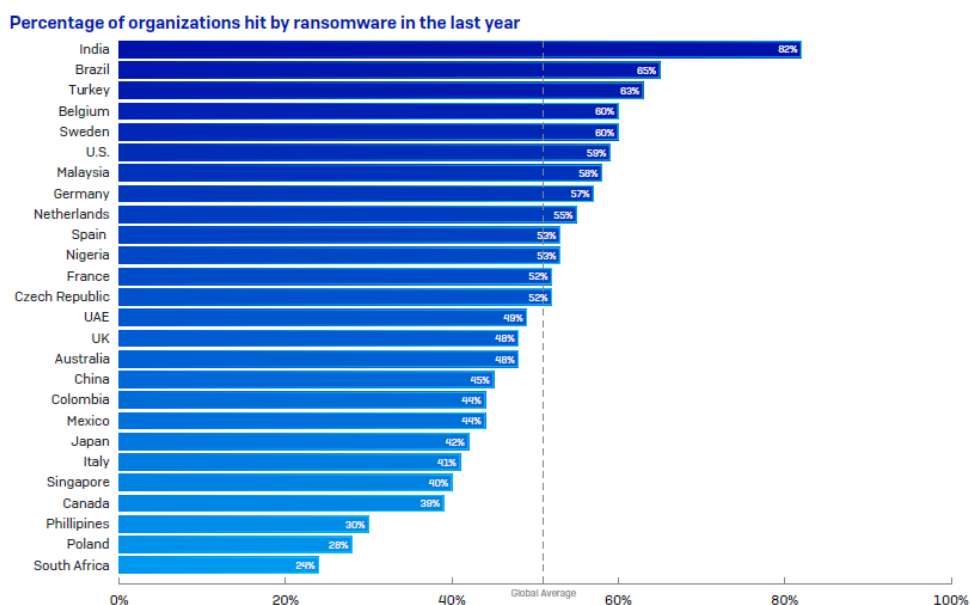
SPAM : GARE AUX ARNAQUES !

LOTTERIE, PETITES ANNONCES OU APPREZ, AUX DOSES, LES PRINCIPALES ARNAQUES PAR MAIL

vous informe

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"]

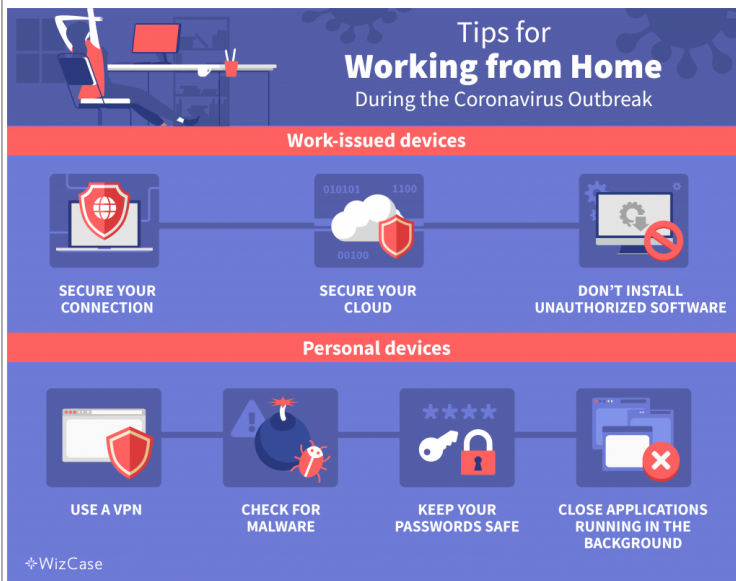
Source : Etude : Payer la rançon multiplie par deux le coût total d'un ransomware

Pour ceux qui continuent le travail à domicile, respectez les cybergestes barrière

| | | | | | |
|--|---|---|--|---|---|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  |  |  |  |  |  |
|  <p>Denis JACOPINI</p> <p>VOUS INFORME</p> <p>L'ÉTI</p> | <p>Pour ceux qui continuent le travail à domicile, respectez les cybergestes barrière</p> | | | | |

Alors que la pandémie mondiale continue à se propager parmi les populations, plusieurs pays ont fermé leurs frontières et suggéraient aux entreprises de recourir au travail à distance. Même si les risques de contagion sont quasiment inexistant, d'autres précautions et des cybergestes barrière sont à respecter.

Restez en sécurité



Comme vous ne savez peut-être pas dans quelle mesure votre environnement de travail assure la sécurité de vos informations, vous risquez de devenir une cible facile pour les hackers une fois que vous serez en confinement ou que vous travaillez à domicile.

Appareils & Équipements de travail

Si vous utilisez un ordinateur de bureau ou un appareil mobile fourni par l'entreprise, il est fort probable que vous soyez déjà muni de quelques éléments de base pour vous protéger. En tant que propriétaire ou dirigeant d'entreprise, vous devrez également vous assurer que les mesures suivantes soient en place pour votre équipe.

1. Sécurisez votre connexion

Si vous n'êtes pas encore installé, demandez à votre responsable informatique de vous fournir un VPN. Il vous aidera à sécuriser votre activité professionnelle. Le wifi public – que vous utilisiez un hotspot local ou que vous partagiez un réseau avec votre voisin – est plus vulnérable que votre propre réseau privé, mais un VPN vous protégera des menaces sur les deux.

2. Sécurisez votre Cloud

Disposer d'une solution de sécurité premium pour le Cloud (CASB) permet de limiter l'accès à vos données dans le Cloud aux seuls membres autorisés de l'équipe.

3. N'installez pas de logiciels non autorisés

Si vous avez apporté votre ordinateur portable de travail à la maison, n'installez aucun logiciel qui ne soit pas lié au travail et n'utilisez pas de clés USB sans être sûr de ce qu'elles contiennent.

Appareils personnels

Mélanger le travail et le plaisir ? Dans certains cas, vous n'avez pas vraiment le choix.

1. Vérifier la présence des malwares

Vérifiez que votre logiciel antivirus est à jour et recherchez tout logiciel malveillant sur votre ordinateur ou votre téléphone portable personnel.

2. Protéger les mots de passe

Utiliser un gestionnaire de mots de passe pour se tenir au courant des meilleures pratiques d'utilisation des différents mots de passe sur le web.

3. Utiliser un VPN

Comme nous l'avons déjà mentionné, un VPN conservera vos informations cryptées pendant toute la durée du confinement – et vous aurez en plus la possibilité d'accéder à l'ensemble de la bibliothèque Netflix dans le monde entier une fois votre journée de travail terminée.

4. Fermer les applications fonctionnant en arrière-plan

N'utilisez pas de logiciels ou d'applications qui ne sont pas en rapport avec le travail, y compris en les laissant s'exécuter en arrière-plan. Évitez également de télécharger de nouvelles applications qui ne sont pas liées au travail pendant cette période.

5. Ne pas enregistrer vos données sans autorisation

Lorsque vous travaillez sur votre ordinateur personnel, évitez de sauvegarder vos données professionnelles, à l'exception de ce qui est absolument nécessaire pour travailler.

6. Garder les choses séparées

Si vous utilisez un ordinateur partagé, créez un espace de travail séparé. Créez un nouvel utilisateur pour l'ordinateur, si possible. Sinon, créez une nouvelle session de navigation avec vos informations spécifiques au travail et pour le travail uniquement – et n'oubliez pas de vous déconnecter à chaque fois !

[L'article complet de l'auteur Chase Williams]

[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 : *5 idées pour travailler à domicile pendant l'épidémie de coronavirus*

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



| | |
|--|--|
|  <p>Denis JACOPINI EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ vous informe</p> | <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 | | | | | |
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LE NET EXPERT .fr</p> |  <p>RGPD CYBER LE NET EXPERT MISES EN CONFORMITE</p> |  <p>SPY DETECTION Services de détection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|  <p>Denis JACOPINI vous informe</p> | | <p>Le prestataire informatique responsable en cas de perte de données par un cryptovirus</p> | | | |

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)...[lire la suite]

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 !

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

| | | | | | |
|---|---|--|---|--|--|
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p> |  <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p> |  <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|---|---|--|---|--|--|



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 prédéfinie 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*

Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

| | | | | | |
|---|--|--|--|---|---|
| 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 detection de logiciels espions |  LE NET EXPERT FORMATIONS |  LE NET EXPERT ARNAQUES & PIRATAGES |
|  Denis JACOPINI EXPERT INFORMATIQUE ASSERMENTE SPECIALISE EN CYBERSECURITE vous informe | Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus | | | | |

Les courriels – qui circulent principalement en Asie pour le moment – prétendent contenir de l’information légitime au sujet du coronavirus.

Le destinataire est invité à cliquer sur une pièce jointe pour obtenir plus d’information. Ceux qui tombent dans le piège permettent involontairement aux pirates d’avoir accès à leurs documents personnels.

IBM dit qu’on s’attend à «voir circuler davantage de courriels malveillants inspirés par le coronavirus dans le futur, alors que l’infection se propagera. Cela se produira probablement aussi dans d’autres langues».

Les pirates informatiques exploitent régulièrement l’actualité et les craintes de la population pour sévir. «Une telle stratégie permet de berner plus de victimes pour qu’elles cliquent des liens malveillants ou ouvrent des fichiers malveillants, accroissant ultimement l’efficacité de la campagne malveillante», peut-on lire dans le rapport...[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 : *Des pirates informatiques profitent du coronavirus pour répandre un logiciel malveillant | HuffPost Québec*