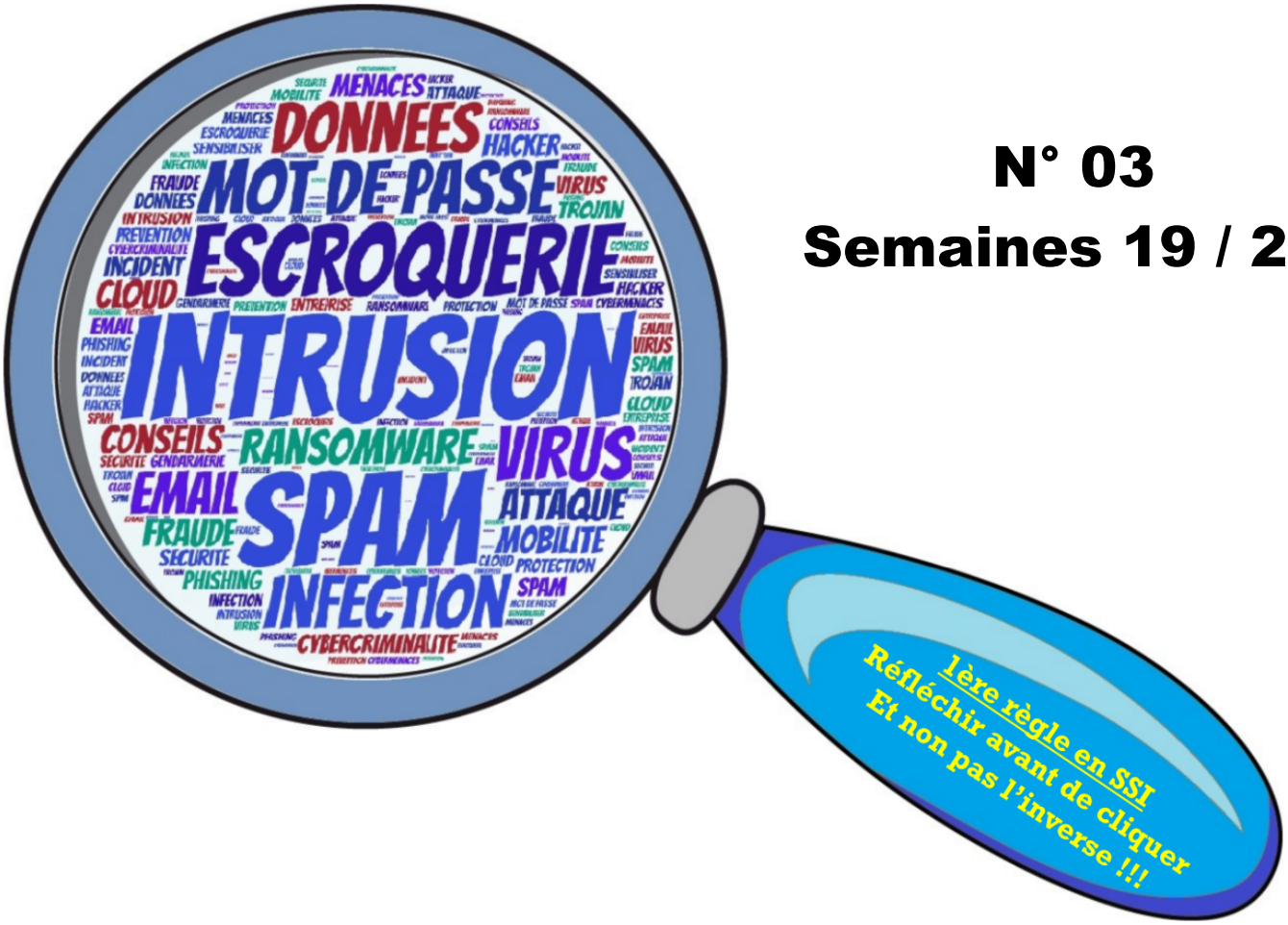
Sécurité économique territoriale

Auvergne - Rhône-Alpes

BULLETIN DE VEILLE CYBER



N° 03

Semaines 19 / 20

IMPORTANT : **Recueilli *EXCLUSIVEMENT* à partir de sources ouvertes, le contenu de ce bulletin est public. Mis à disposition à titre d'*information*, de *prévention* et de *sensibilisation*, les articles présentés ne subissent aucune action éditoriale et ne saurait en aucun cas engager la responsabilité du rédacteur du présent document.**

Pour consulter les articles dans leur intégralité, cliquer sur le lien « *source* ».

SOMMAIRE

I - L'INFO DE LA QUINZAINE

II - ESCROQUERIES & ARNAQUES

III - RANSOMWARES

IV - CYBERMENACES, MALWARES, VIRUS...

V - VIE DE L'ENTREPRISE

L'INFO DE LA QUINZAINE

La nouvelle formation en ligne de l'ANSSI met la cybersécurité à la porté de tous

La formation et la sensibilisation des Français à la sécurité du numérique est un enjeu majeur. Pour y répondre, l'Agence National Sécurité des Systèmes d'Information lance son premier cours en ligne, le MOOC SecNumacadémie, qui rend la cybersécurité accessible à tous.

Étudiants, salariés, dirigeants d'entreprise ou particuliers… plus que jamais, la sécurité du numérique est l'affaire de tous. Pour mieux informer et sensibiliser, la formation en ligne SecNumacadémie propose des contenus pédagogiques, adaptés à des publics variés, afin qu'ils deviennent à leur tour acteurs de la sécurité du numérique dans un environnement professionnel. Ces bonnes pratiques et réflexes indispensables s'appliquent et s'adaptent également aux particuliers, dans un usage plus personnel du numérique.

L'objectif de SecNumacadémie est de permettre à tous d'être initiés à la cybersécurité ou d'approfondir leurs connaissances, afin de pouvoir agir efficacement sur la sécurité de leurs systèmes d'information (SSI) au quotidien.

-> Pour lire la suite et vous inscrire à la formation de l'Agence Nationale SSI

ESCROQUERIES - ARNAQUES

Ils ont escroqué des millions d'euros en se faisant passer pour Le Drian

http://www.liberation.fr/planete/2017/05/12/ils-ont-escroque-des-millions-d-euros-en-se-faisant-passer-pour-le-drian_1569090

Les escrocs avaient installé une réplique parfaite du bureau du ministre Jean-Yves Le Drian (ici en avril 2014) pour convaincre leurs victimes de payer. Photo Joël Saget. AFP

Installés en Israël, des hommes qui usurpent l'identité du ministre de la Défense réclament de l'argent à des entreprises ou même à des chefs d'État.

Arnaques sur Internet : les astuces pour les repérer

http://www.phonandroid.com/arnaques-internet-astuces-reperer.html

Fréquemment, Internet vous propose des placements financiers alléchants, qui vous font croire à un rendement optimal en peu de temps. Mais bien souvent, ces annonces dissimulent des arnaques qui peuvent s'avérer dangereuses pour votre porte-monnaie. Des astuces existent pour les repérer et les éviter.

Sur Internet, on vous propose souvent des produits financiers à 10%, 15% ou encore 20% alors que la plupart des produits de placement ordinaires comme le PEL ou l'assurance-vie rémunèrent à 1,5% ou 2%. Il faut alors se méfier des offres alléchantes que l'on peut plaquer sous vos yeux sur le Web. Les produits financiers miracles n'existent pas, alors restez vigilants.

L'arnaque à la clé USB continue de se propager, attention !

http://www.planet.fr/high-tech-larnaque-a-la-cle-usb-continue-de-se-propager-attention.1354642.1506.html

Une clé USB déposée dans votre boîte aux lettres et ensuite branchée sur votre ordinateur va permettre à des malfaiteurs de voler vos données personnelles. La gendarmerie de Charente met à son tour en garde.

"Prudence est mère de toutes les vertus...", rappellent les autorités. Nous vous mettions en garde il y a deux mois face à une nouvelle escroquerie dite "à la clé USB". Mais celle-ci continue de faire des victimes. La gendarmerie de Charente a donc publié à son tour il y a deux semaines une nouvelle mise en garde sur sa page Facebook pour éviter au maximum les risques.

ESCROQUERIES – ARNAQUES

Compte bancaire : 5 conseils pour éviter le piratage et les arnaques

http://www.cbanque.com/actu/62836/compte-bancaire-5-conseils-pour-eviter-le-piratage-et-les-arnaques

Usurpation d'identité, phishing, malwares : nombreuses sont les menaces qui pèsent, à l'âge du numérique, sur vos comptes bancaires. 5 conseils pour prévenir les piratages, et éviter d'être taxé de négligence par votre banque.

Attention aux courriels et sites frauduleux

http://www.leprogres.fr/faits-divers/2017/05/18/attention-aux-courriels-et-sites-frauduleux

Votre Caisse d'allocations familiales (CAF) vous met en garde contre le « phishing » : des messages frauduleux que vous avez peut-être reçus, par courriel ou par téléphone (SMS ou message vocal).

Votre CAF ne demande jamais votre numéro de carte de crédit, ni sur un site internet, ni par courriel, ni au téléphone.

Pour être sûr que vous consultez le site de votre CAF et non un site pirate qui imite celui de votre CAF, il suffit de saisir manuellement l'adresse http://www.caf.fr dans votre navigateur.

RANSOMWARES

Près de 100 pays touchés par une cyberattaque internationale

http://www.lefigaro.fr/secteur/high-tech/2017/05/12/32001-20170512ARTFIG00306-une-cyberattaque-d-envergure-frappe-des-hopitaux-britanniques.php

L'attaque informatique massive internationale affectant une centaine de pays et des dizaines d'entreprises et d'organisations est «d'un niveau sans précédent», a déclaré samedi l'Office européen des polices Europol.

Plus les heures passent, plus les informations tombent. Samedi matin, l'Office européen des polices Europol a déclaré que la cyberattaque internationale qui touche depuis vendredi une centaine de pays et des dizaines d'entreprises et d'organisations est «d'un niveau sans précédent». «L'attaque (...) exigera une investigation internationale complexe pour identifier les coupables», a indiqué Europol dans un communiqué. Le Centre européen de cybercriminalité (EC3) de l'Office européen des polices «collabore avec les unités de cybercriminalité des pays affectés et les partenaires industriels majeurs pour atténuer la menace et assister les victimes», a-t-il ajouté.

Cyberattaque WannaCry, ce n'est qu'un début !

http://www.zebulon.fr/actualites/16531-cyberattaque-wannacry-ce-n-est-qu-un-debut.html

Vendredi et une bonne partie du weekend, un grand nombre d'entreprises ont été la cible d'une vaste cyberattaque menée à l'aide d'un malware baptisé WannaCry ou Wannacrypt.

Comme avec tous les ransomwares, l'objectif des pirates derrière cette attaque est de soutirer une somme d'argent, dans le cas de cette campagne, de 300 dollars pour débloquer les PC cryptés.

Cyberattaque massive : quelle attitude adopter face à un «ransomware»

http://m.leparisien.fr/high-tech/cyberattaque-massive-quelle-attitude-adopter-face-a-un-rancongiciel-13-05-2017-6944841.php

Des milliers d'ordinateurs sous Windows sont la cible depuis vendredi d'un logiciel, WCry, qui menace de ne pas rendre les données sauf versement d'une rançon.

Les «rançongiciels» («ransomware» en anglais) promettent de libérer vos données contre le paiement d'une rançon. Quelques conseils pour se prémunir contre ce type d'attaques ou y faire face.

RANSOMWARES

Cyberattaques : Renault touché, une enquête ouverte en France

http://www.leprogres.fr//faits-divers/2017/05/13/renault-touche-par-la-vague-de-cyberattaques-internationales

Une vague de cyberattaques simultanées a touché des dizaines de pays dans le monde, avaient alerté vendredi les autorités américaines et britanniques.

Ce samedi, on apprend que l'entreprise française Renault est impactée. Le parquet de Paris a décidé d'ouvrir une enquête en France.

Wannacry : Le point au jour 4

http://www.informatiquenews.fr/wannacry-point-jour-4-51990

La société Ivanti spécialisée en intégration et en automatisation des tâches IT critiques fait le point le point sur l'attaque Wannacry et propose quelques conseils.

Nom du malware (et toutes les variantes signalées, dont certaines sont plus anciennes mais apparentées) :

WannaCrypt, Wana Decrypt0r 2.0, WanaDecryptor, WannaCry, WanaCrypt0r, WCrypt, WCRY

Ransomware WannaCry : son impressionnant bilan en huit chiffres

http://www.01net.com/actualites/ransomware-wannacry-son-impressionnant-bilan-en-huit-chiffres-1164307.html

Depuis vendredi, de nombreux PC sont les victimes d'un ransomware. 3 jours après, quel est le premier bilan du virus WannaCry ?

Si la propagation du ransomware WannaCry a pu être mitigée in extremis ce week-end, de nombreuses variantes sont en préparation et pourraient même déjà être en cours de propagation. Au moment où de nombreuses entreprises rentrent de week-end et pourraient être victimes de ce virus, qui chiffre l'ordinateur et exige le paiement d'une rançon pour un déverrouillage, petit bilan chiffré de cette attaque informatique sans précédent.

« Exaspérés » par WannaCrypt, des experts en sécurité montent le collectif Résistance Cyber

https://www.nextinpact.com/news/104288-exasperes-par-wannacrypt-experts-en-securite-montent-collectif-resistance-cyber.htm?skipua=1

Visant des systèmes pour partie obsolètes, le ransomware WannaCrypt a touché nombre d'institutions publiques et de systèmes industriels. Une situation qui doit alarmer les décideurs, selon le collectif Résistance Cyber, qui veut revoir la vision de la sécurité pour la focaliser sur les bonnes pratiques.

Si le ransomware WannaCrypt n'est pas un électrochoc suffisant, Résistance Cyber veut forcer le changement dans la sécurité informatique. « Collectif spontané » monté hier (dont le nom fera sourire certains), il est composé de spécialistes dans le domaine de la cybersécurité, qui réclament de revoir le modèle de sécurité des entreprises en France.

Sécurité informatique : Mieux comprendre les dangers autour des cyberattaques

http://www.cegid.com/fr/blog/cybersecurite-informatique-dangers/

La sécurité des données est un sujet à mettre au centre des préoccupations de l'entreprise. La recrudescence des cyberattaques, avec dernièrement le ransomware LOCKY et actuellement WANNACRY le rappelle douloureusement, une attaque qui touche particulièrement la France.

WannaCrypt : le racket mondial n'a pour l'instant pas rapporté grand-chose

http://www.numerama.com/politique/258476-wannacrypt-la-campagne-mondiale-de-racket-na-pas-rapporte-grand-chose.html

Depuis vendredi 12 mai, WannaCrypt se répand dans le monde entier. Une analyse des versements exigés par le rançongiciel montre que les sommes obtenues sont assez modérées au regard de l'ampleur de la campagne de racket.

Ça ne paie pas toujours d'être un criminel 2.0. En tout cas, si c'est la perspective d'un enrichissement facile et rapide qui a motivé le développement de WannaCrypt, c'est raté. En effet, malgré une campagne de racket d'une ampleur inédite (le rançongiciel a infecté en quelques jours 200 000 postes informatiques répartis dans 150 pays, selon Europol), les paiements restent assez rares.

Limitez les risques et évitez les attaques par ransomware

https://www.proximus.be/fr/id_b_cl_ransomware_attacks/entreprises-et-secteur-public/decouvrir/blog/one-magazine/news/cybersecurite.html

Une nouvelle souche du Ransom.CryptXXX (WannaCry) a commencé à se propager vendredi 12 mai, touchant de nombreuses organisations surtout en Europe. Comment cette attaque s'est-elle propagée si rapidement et que pouvez-vous faire pour y échapper ?

RANSOMWARES

Accepter l’extorsion par ransomware encourage les criminels

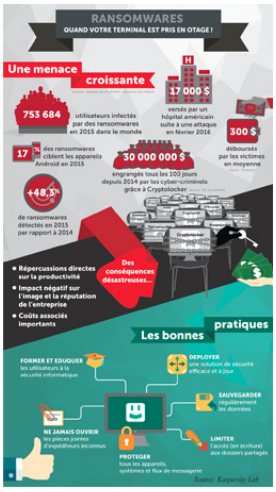
http://globbsecurity.fr/accepter-lextorsion-ransomware-encourage-criminels-41598/

Si l’attaque WannaCry a mis abruptement le public au fait des Ransomware, certains oublient que les cybercriminels exploitant les ransomware ont extorqué plus de 1 milliard de dollars aux victimes l’année dernière et que près de 47 % des entreprises ont déjà subi au moins une attaque de type ransomware.

Bien qu’il soit relativement tentant de payer la rançon, c’est un mauvais pari : une victime sur cinq qui paie ne reçoit jamais le remède promis et le paiement ne contribue pas à dissuader l’attaquant d’effectuer d’autres attaques. Accepter l’extorsion par ransomware encourage les criminels et contribue à financer un peu plus leurs efforts de développement. Vous devez soit mettre en place une défense efficace, soit vous résoudre à devenir une victime répétée.

Les dessous de l’une des plus grosses cyberattaques

http://leconomiste.com/article/1012453-les-dessous-de-l-une-des-plus-grosses-cyberattaques



L’outil malveillant a été développé par la NSA avant de fuiter sur le deepweb. Il suffit de mettre à jour son système d’exploitation pour éviter d’être infecté. Le ransomware, en libre accès dans la sphère cybercriminelle, risque de réapparaître sous une autre forme

Ransomware WannaCry - Seuls les négligents ont été touchés

http://www.afjv.com/news/7551_ransomware-wannacry-seuls-les-negligents-ont-ete-touches.htm

Plus de 20.000 victimes, des centaines de milliers d'ordinateurs infectés dans 150 pays, une usine Renault fermée en France. La cyber attaque massive du weekend dernier fait la une des journaux dans le monde entier. Au-delà du battage médiatique, le principal enseignement que l'on peut tirer de cet événement est que seuls les négligents ont été touchés.

En effet, il semble qu'aucune entreprise ou organisation ayant mis en place une politique de cyber sécurité strictement mise à jour n'ait été touchée.

RANSOMWARES

Coût de WannaCrypt : faut-il mettre à jour ou subir des attaques ?

http://globbsecurity.fr/cout-de-wannacrypt-faut-mettre-a-jour-subir-attaques-41627/

Le ransomware « WannaCrypt » fait beaucoup parler de lui ces derniers jours : plus de 200 000 victimes dans 150 pays, des milliers de dollars récoltés… Se propageant via une vulnérabilité Microsoft Windows, comment une attaque d'une telle ampleur a-t-elle été rendue possible ?

Cette attaque n'est pas nouvelle dans son genre, mais sa portée est spectaculaire comparée aux autres menaces. Pour autant, cela n'est pas surprenant. Les techniques utilisées par les pirates évoluent aussi rapidement que les technologies de cybersécurité.

L'originalité de cette menace repose sur sa double fonction. Agissant comme un ransomware par la demande de rançon, WannaCrypt dispose des capacités d'un ver informatique, ce qui lui permet de se propager par lui-même.

L'homme qui a freiné la propagation du logiciel malveillant qui a infecté 150 pays a 22 ans

http://www.slate.fr/story/145566/stop-virus-malware-tech-pays

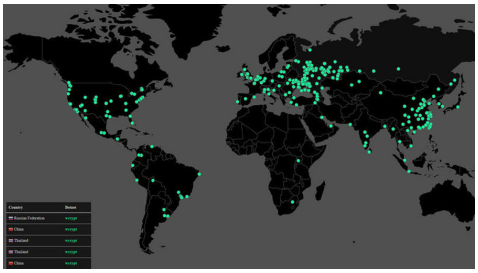
Il a accidentellement stoppé la progression en achetant un nom de domaine. Mais les craintes de nouvelles infections demeurent dans de nombreux pays alors que la semaine recommence.

Une nouvelle cyberattaque géante en cours

http://www.ledauphine.com//france-monde/2017/05/17/une-nouvelle-cyberattaque-geante-en-cours

Une nouvelle cyberattaque de grande ampleur est en cours et touche des centaines de milliers d'ordinateurs dans le monde dans le but de créer et récupérer de la monnaie virtuelle à l'insu des utilisateurs, alertent des experts.

L'attaque "Adylkuzz"



Après l'attaque au "rançongiciel" WannaCry repérée vendredi, "les chercheurs de Proofpoint (société de sécurité informatique, NDLR) ont découvert une nouvelle attaque liée à WannaCry appelée Adylkuzz. Elle utilise de manière plus furtive et à des fins différentes les outils de piratage récemment divulgués par la NSA et la vulnérabilité désormais corrigée de Microsoft", a expliqué le chercheur Nicolas Godier, expert en cybersécurité de Proofpoint.

"On ne connaît pas encore l'ampleur des dégâts mais des centaines de milliers d'ordinateurs" pourraient avoir été infectés, a précisé Robert Holmes, vice-président produit chez Proofpoint, qui assure que l'attaque est "de bien plus grande envergure" que WannaCry.

CYBERMENACES – MALWARES - VIRUS

Logiciels malveillants : on va encore pleurer

http://m.trends.levif.be/economie/politique-economique/logiciels-malveillants-on-va-encore-pleurer/article-opinion-662105.html

Les entreprises sont de plus en plus victimes de logiciels malveillants. Au lieu de traiter cela comme un sujet technique réservé à la direction informatique, la direction générale ferait bien de s'en saisir et d'avoir une véritable prise de conscience, car ces attaques vont empirer.

Piratage : 560 millions de login et mots de passe volés se retrouvent sur le net

http://www.phonandroid.com/piratage-millions-login-mots-de-passe-voles-net.html

Un nouveau piratage massif vient de déboucher sur la mise en ligne de 560 millions de login et mots de passe venant d'un site qui n'est pas pour l'instant connu. L'information pourrait provenir de précédents piratages de LinkedIn, LastFM, Tumblr et/ou Dropbox. Si vous avez un compte sur l'un de ces services et n'avez pas changé de mot de passe depuis un certain temps, c'est peut-être le moment.

Prenez garde aux cyberattaques !

http://www.usinenouvelle.com/

La cybersécurité est essentielle, mais par où commencer ? Voici cinq principes fondamentaux pour vous aider à faire le premier pas.

Il est loin le temps où les entreprises pouvaient se contenter d'un antivirus et d'un firewall pour protéger leur système d'information. Les menaces ont évolué, les surfaces d'attaques ont augmenté et les systèmes se sont complexifiés. Le coût des cyberattaques, qui représente aujourd'hui 450 milliards de dollars par an dans le monde, dépassera les 2000 milliards en 2019, d'après le gouvernement américain. La nécessité de se protéger est donc plus forte que jamais, que l'on soit un cabinet d'architectes, une ETI industrielle ou un grand groupe.

Voici cinq conseils pour partir sur de bonnes bases.

La cybercriminalité ne cesse de se renforcer

http://www.assurbanque20.fr/la-cybercriminalite-ne-cesse-de-se-renforcer/

Selon cette étude, 8 entreprises sur 10 ont subi au moins une tentative de fraude en 2016 ; un quart des entreprises ont subi plus de 10 tentatives de fraude l'an dernier. La fraude au « faux président » est la plus citée (59 %), suivi de la cyberattaque (57 %). Au total 200 directeurs financiers ont été passées au crible et le principal enseignement est que le risque de fraude continue de planer sur les entreprises en France.

Ainsi, plus de 8 entreprises sur 10 déclarent avoir été victimes d'au moins une tentative de fraude au cours de l'année 2016.

La menace s'intensifie, et les entreprises françaises sont ciblées en continu : 25 % d'entre elles ont subi plus de 10 tentatives de fraude en 2016. Plus de 8 entreprises sur 10 déclarent avoir été victimes d'au moins une tentative de fraude au cours de l'année 2016. La menace s'intensifie, et les entreprises françaises sont ciblées en continu : 25% d'entre elles ont subi plus de 10 tentatives de fraude en 2016.

Nouveau botnet de caméra IP

http://www.toolinux.com/Nouveau-botnet-de-camera-IP

Le malware Persirai crée actuellement un nouveau botnet de plus de 100.000 caméras IP.

Trend Micro vient de découvrir un nouveau malware. Celui-ci, nommé Persirai, infecterait plus de 1000 modèles de caméras IP d'un constructeur chinois, pour un total d'au moins 100.000 appareils. C'est ce qu'a détecté Shodan, le moteur de recherche de vulnérabilité de la société de sécurité.

Cybersécurité: des responsables américains se méfient de Kaspersky

http://www.lefigaro.fr/flash-actu/2017/05/12/97001-20170512FILWWW00003-cybersecurite-des-responsables-americains-se-mefient-de-kaspersky.php

De hauts responsables de la sécurité et du renseignement américains ont fait publiquement part ce jeudi de leurs doutes concernant le géant de la sécurité informatique Kaspersky Lab, en raison de ses liens présumés avec Moscou.

Google Docs visé par une campagne de phishing

http://www.solutions-numeriques.com/google-docs-vise-par-une-campagne-de-phishing/

Vous possédez un compte Google ? Gare. L'entreprise met en garde ses utilisateurs contre une tentative de phishing par mail .
Plusieurs utilisateurs ont reçu un mail les invitant à modifier un Google Docs. En cliquant sur un lien, les internautes accèdent à une page d'authentification, qui n'est qu'un leurre pour obtenir contacts et mails. Dans un tweet du 3 mai du compte Gmail, Google met en garde ses utilisateurs : ne cliquez pas et signalez le comme hameçonnage, indique-t-il.

VIE DE L'ENTREPRISE

Inspection du travail: que dit le récent code de déontologie ?

http://lentreprise.lexpress.fr/rh-management/droit-travail/inspection-du-travail-que-dit-le-code-de-deontologie_1901043.html

Pour un contrôle, l'inspecteur du travail a le droit d'entrer librement dans l'établissement, à toute heure du jour ou de la nuit. (Getty Images).

Les employeurs ne sont pas à l'abri d'un contrôle. Dans quel cadre une visite est-elle possible? Quelle est l'étendue des pouvoirs de l'inspecteur? Éclairage.

Pause déjeuner: les obligations de l'entreprise allégées

http://lentreprise.lexpress.fr/rh-management/droit-travail/pause-dejeuner-les-obligations-de-l-entreprise-allegees_1907121.html

Les entreprises dont moins de 25 salariés sont concernés par la pause repas sur le lieu de travail voient leur démarche de déclaration d'un emplacement de restauration auprès de l'inspection du travail simplifiée. (Getty Images)

Manger rapidement au bureau est une pratique répandue, mais réglementée. Un récent décret assouplit les obligations de l'employeur en la matière.

Consultation d'e-mails par l'employeur : rappel des principes

http://www.usine-digital.fr/droits-numeriques

Tribune : Toutes les deux semaines, les avocats de CMS Bureau Francis Lefebvre nous aident à décrypter la loi et les nouvelles réglementations afin de mieux appréhender l'impact du numérique sur l'activité des entreprises en matière de droit social et de propriété intellectuelle. Aujourd'hui, Rodolphe Olivier, Avocat associé, Département social, fait une mise au point sur la consultation des e-mails par les employeurs.

VIE DE L'ENTREPRISE

Données confidentielles de l'entreprise : la moitié des salariés a des comportements à risque

http://www.solutions-numeriques.com/donnees-confidentielles-de-lentreprise-la-moitie-des-salaries-a-des-comportements-a-risque/

Alors que la mise en application du règlement européen sur la protection des données personnelles sera imposée dans un an, savez-vous ce que font les salariés avec les informations confidentielles ? Êtes-vous sûr de leur sécurité ? Si oui, vous avez tort.

Le fait religieux dans l'entreprise : quelle pratique ?

http://www.daf-mag.fr/Thematique/social-rh-1032/Breves/Tribune-fait-religieux-dans-entreprise-quelle-pratique-316905.htm?utm_source=DAF_17_5_2017&utm_medium=email&utm_campaign=newsletter&

Voile islamique mais pas que : les arrêts rendus le 14 mars 2017 sont une bonne nouvelle pour les employeurs français : ils fournissent des orientations pratiques certaines aux entreprises pour éviter d'être sanctionnées sur la base du principe de discrimination.

Le fait religieux dans l'entreprise : quelle pratique ? Rendus le 14 mars 2017, les arrêts de la CJUE fournissent des orientations pratiques certaines aux entreprises pour éviter d'être sanctionnées sur la base du principe de discrimination. Car l'employeur est souvent pris en étau entre la perte de ses clients et le licenciement de salariés licenciés pour refus d'obtempérer et dès lors encourt le risque de se voir accusé de discrimination.