La France nomme un « administrateur général des données », le 1er en Europe

La France nomme un « administrateur général des données »

Nous l'avions annoncé le 26 mai dernier :http://www.lenetexpert.fr/france-nome-chef-protection-donnees-personnelles-les-administrations-cdo-chief-data-officer/
Henri Verdier vient d'être nommé administrateur général des données, la première fonction de ce type créée dans un pays d'Europe, afin de faire entrer le service public dans l'ère des données, selon un décret publié vendredi.

Le responsable, qui conserve ses fonctions de directeur d'Etalab, la mission chargée de l'ouverture des données publiques, est placé sous l'autorité du Premier ministre au sein du secrétariat général pour la modernisation de l'action publique.
« L'État doit savoir utiliser ses données pour s'améliorer, pour faire des économies, pour mieux piloter certaines politiques publiques », a expliqué Henri Verdier à l'AFP au cours d'une visite de start-up vendredi, avec Thierry Mandon, secrétaire d'État chargé de la Réforme de l'État.
« Il faut avoir des +data scientists+, des gens qui ont la culture de la donnée dans l'État, on va en recruter quelques uns pour faire de l'expérimentation. Il faut être sûr que celui qui prend une décision ait vraiment la donnée. Il faut être sûr qu'on les recueille bien », a-t-il poursuivi.
M. Verdier, membre fondateur en 2006 du pôle de compétitivité Cap Digital, sera chargé d'assurer l'ouverture des données, leur circulation et leur exploitation au sein de l'administration afin d'améliorer l'action publique. Il pourra aussi proposer au Premier ministre une position française dans les négociations internationales sur la politique de la donnée.
Thierry Mandon a souligné « l'intérêt économique » de l'ouverture des données publiques lors de sa visite dans les start-up Fivebyfive et Snips, spécialisées dans le traitement de la donnée.
Fivebyfive a mis au point des applications pour la SNCF lui permettant d'adapter son réseau de gares aux personnes à mobilité réduite, tandis que Snips a construit notamment un modèle permettant de prédire les risques d'accidents de la route à base de données comme la météo, la date, la topographie…

La France est le premier pays à mettre en place un administrateur général des données au niveau national, alors que cette fonction de « chief data officer » a été créée par certaines villes comme New York ou San Francisco ou entreprises comme Yahoo, CityGroup, Ogilvy.

Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://lentreprise.lexpress.fr/actualites/1/actualites/la-france-nomme-un-administrateur-general-des-donnees-le-1er-en-europe_1577573.html

---

Droit à l'oubli : des directives édictées par le G29 en préparation

Droit à l'oubli : des directives édictées par le G29 en préparation

Réunis en assemblée cette semaine, les différentes autorités de protections des données personnelles européennes ont commencé à travailler sur les directives d'applications du droit à l'oubli. Pour l'instant, chaque moteur de recherche interprète ce droit à sa manière.

Si la loi issue de l'arrêt rendu en mai par la CJUE ne fait plus débat, son application reste encore problématique. Dans les faits, cet arrêt met en place un droit à l'oubli, garantissant aux citoyens des moyens de recours afin de faire déréférencer des informations les concernant et qu'ils ne jugent plus valides ou discriminantes.
Mais si tout le monde s'accorde plus ou moins sur cette décision, la mise en place effective de ce droit fait débat. Google a ainsi rapidement proposé un formulaire afin de transmettre les demandes de déréférencement relatives au droit à l'oubli mais la Cnil voit d'un mauvais œil cette approche unilatérale, qui laisse à Google le soin d'interpréter à sa guise l'arrêt de la CJUE et de s'imposer comme intermédiaire unique.

Axelle Lemaire, secrétaire d'Etat au Numérique, expliquait d'ailleurs à ZDNet.fr que ce modèle « ne lui convenait pas » tout en plaidant pour une redéfinition du rôle de la Cnil.

Une réunion des différentes Cnil européenne avait lieu mercredi et jeudi. A cette occasion, les participants ont annoncé la préparation de directives afin de statuer sur les cas litigieux. Rien de définitif pour le moment, le projet est encore à l'étape de l'élaboration, mais le G29 promet qu'un document complet sera présenté pour le mois de novembre.

Dura lex, sed lex
L'objet de ces directives sera de donner une « boite à outils » pour jauger les cas jugés complexes, c'est-à-dire les cas refusés par Google. Pour l'instant en effet, Google est seul à juger de la validité des demandes de déréférencement qui lui sont adressées. Ces outils se présenteront sous deux formes : d'une part une classification des cas en différentes catégories et d'autre part une compilation des différents arbitrages rendues par les autorités nationales, afin de donner des références pour l'application des jugements futurs.
Au total, 90 réclamations ont été déposées auprès des différentes autorités nationales suite à un refus de déréférencement de la part de Google, dont une vingtaine en France. Google avait annoncé en juillet avoir reçu plus de 90.000 demandes de déréférencement mais ce chiffre progresse et Reuters rapporte que Google aurait déjà traité plus de 120.000 demandes.Nous avons contacté les porte-paroles de Google France à propos de ces chiffres mais nous n'avons pas encore reçu de réponse de leurs part.
Les membres du G29 ont également rencontré différents éditeurs de presse, inquiets des conséquences du déréférencement de leurs articles vis-à-vis du droit à l'information. Outre l'opposition entre Google et les différentes autorités européennes autour de l'application de ce nouveau droit, le débat reste ouvert afin de trouver le « bon équilibre » entre protection des données personnelles et droit légitime à l'information pour le grand public.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/droit-a-l-oubli-des-directives-edictees-par-le-g29-en-preparation-39806625.htm
Par Louis Adam | Vendredi 19 Septembre 2014

Home Depot : finalement 56 millions de cartes bancaires piratées

Home Depot : finalement 56 millions de cartes bancaires piratées

Début septembre, l'enseignement américaine Home Depot révélait avoir observé une activité inhabituelle concernant les données de paiement de ses clients avant de reconnaître une intrusion informatique.

Home Depot expliquait ainsi que tout client ayant utilisé, depuis le mois d'avril, une carte bancaire pour régler un achat dans l'un de ses magasins aux Etats-Unis et au Canada est potentiellement concerné par le vol de ces données de paiement.
Le groupe ne chiffrait pas le nombre de clients affectés ni le détail exact des données personnelles compromises. Le New York Times évoquait le nombre de 60 millions de cartes de paiement compromises.

EMV
Bingo, Home Depot indique aujourd'hui que ce sont 56 millions de cartes bancaires ont été « mises en péril ». De quoi constituer un nouveau triste record en la matière, jusqu'ici détenu par Target (40 millions de cartes de paiement compromises).
D'ailleurs, comme pour Target, il semble que les pirates aient exploité une variante du programme malveillant BlackPOS installé dans le système de paiement de l'entreprise.
Seule bonne nouvelle, Home Depot estime qu'à ce stade de l'enquête aucune preuve ne permet d'établir que les codes PIN des cartes bancaires compromises figurent également parmi les données dérobées. Mais cette protection est assez peu utilisée aux Etats-Unis…
A la suite de cette intrusion informatique, dont l'ampleur doit encore être précisée, Home Depot a fait savoir qu'il déploierait sur l'ensemble de ses magasins, d'ici à octobre 2015, la technologie EMV de paiement pour cartes à puce. Ce standard international, en vigueur notamment en France, apporte en principe une sécurité accrue des transactions et contribue donc à réduire la fraude.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-finalement-56-millions-de-cartes-bancaires-piratees-39806615.htm

---

Droit à l'oubli : Google

continue ses discussions, la Cnil veut traiter des refus

Droit à l'oubli : Google continue ses discussions, la Cnil veut traiter des refus

Google continue son tour des capitales européennes et mène des discussions autour de l'application du droit à l'oubli pour tous. De son côté, le groupement des autorités chargées de la protection des données personnelles édite un registre commun des demandes de déréférencement refusées par les moteurs.

Le G29, le groupement européen de l'ensemble des autorités chargées de la protection des données personnelles (en France la Cnil) avance sur le dossier du droit à l'oubli. Le collectif annonce avoir mis en place des référents, dans chaque pays, dont la tâche sera de dresser des pratiques communes pour traiter les demandes de déréférencement, en particulier les refus des moteurs de recherche.

Le réseau mis sur pied par le G29 aura la charge d'éditer un registre commun des suites données aux plaintes. Il devra ainsi mettre en place un tableau de bord destiné à coordonner leurs actions en cas de refus des moteurs de recherche. La Cnil indique par exemple avoir déjà reçu « plusieurs dizaines de plaintes ».
Pour rappel, cette procédure de déréférencement est née suite à la publication en mai dernier d'une décision de la Cour de justice de l'Union européenne. La juridiction estimait qu'une personne peut être fondée à demander à ce qu'un moteur de recherche déréférence des liens dirigeant vers des informations la concernant.
La Cour ne consacrait toutefois pas un droit absolu à l'oubli. Elle relevait l'importance de « rechercher un juste équilibre entre cet intérêt et les droits fondamentaux de la personne concernée, en particulier le droit au respect de la vie privée et le droit à la protection de données à caractère personnel ». Le déréférencement peut donc être refusé si le public justifie d'un « intérêt prépondérant » à accéder à ces informations.
De son côté, Google mène actuellement des réunions publiques dont le but est de trouver un « équilibre entre le droit des personnes à l'oubli et le droit à l'information du public ». Après Madrid et Rome, ce rendez-vous doit atteindre Paris à la fin du mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/entreprises/google/actualite-728183-droit-oubli-google-discute-cnil.html

Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

	Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

Après trois jours de débat, l'Assemblée nationale a adopté en première lecture le projet de loi visant à lutter contre le terrorisme. Parmi les différents articles, le polémique blocage administratif des sites faisant l'apologie du terrorisme a été voté par les députés.

C'est un hémicycle bien vide qui s'est prononcé sur le projet de loi contre le terrorisme aujourd'hui : au moment de l'adoption du texte dans son ensemble, une trentaine de députés seulement étaient présents pour voter. Ce texte, soutenu par le ministre de l'Intérieur Bernard Cazeneuve et par le rapporteur désigné, le député PS Sébastien Pietrasanta, a donc été adopté sans difficulté. Il doit encore obtenir l'approbation du Sénat avant de repasser au Palais Bourbon puis d'être ratifié par le président de la République.
Comme nous l'expliquions lundi, Bernard Cazeneuve appelait à un « consensus » autour de ce texte qui vise à lutter contre les nouvelles formes d'enrôlements et de propagandes terroristes, notamment via internet et dans les prisons françaises. Si l'objet du texte n'a en effet pas trop souffert de contradiction, on a pu voir une offensive de la droite qui juge le texte encore trop faible face à la menace qu'il entend combattre.

Lutter contre le terrorisme et au passage, réguler Internet
Si le texte a de lourde implication pour les droits fondamentaux des citoyens, celui-ci n'est pas pour autant sans conséquence pour internet. En effet l'article 4 du texte punit donc de 5 ans d'emprisonnement et d'une forte amende le fait d'utiliser Internet pour faire la promotion du terrorisme. La particularité de cet article est de considérer la diffusion via Internet comme une circonstance aggravante : lorsque l'incitation est faite sur un site web public, au vu et au su de tous, la condamnation pourra monter jusqu'à 7 ans et l'amende à 100.000 euros.

Conséquence logique, l'Assemblée a également entériné le blocage administratif (sans décision de justice donc), véritable serpent de mer des lois relatives à Internet. L'article 9, voté jeudi 18 septembre, a fait l'objet de nombreuses critiques de la part de parlementaires de tout bord, notamment Laure de la Raudière et Lionel Tardy du coté de l'UMP ou encore Patrick Bloch et Corinne Erhel chez les socialistes.
Cette mesure « est une erreur et je vous invite, je nous invite, à ne pas la commettre », a lancé Christian Paul (SRC). « Faut-il faire reculer encore la liberté, contre le terrorisme ? » s'interroge de son côté Lionel Tardy, « la France s'engage à petits pas dans la direction de la NSA ».

Pas une volte face ?
Face à ces critiques, le rapporteur Pietrasanta a fait valoir plusieurs gardes fous mis en place pour éviter les dérives : il faudra d'abord passer par l'éditeur et l'hébergeur afin de faire retirer les contenus problématiques, et le blocage ne sera mis en place que dans les cas ou les premiers recours n'auront rien donné. De plus, une personnalité qualifiée sera nommée pour jauger de la conformité de ces blocages. Reste le risque de surblocage, évoquée par la députée EELV Isabelle Attard qui cite en exemple le récent cas australien de blocage hasardeux de 250.000 sites.
Bernard Cazeneuve est donc revenu sur la méthode de blocage, expliquant que le blocage par DNS, jugé plus précis, serait privilégié mais que la méthode ne serait pas inscrite dans la loi, préférant attendre de fixer cet aspect là par décret.
La volte face du PS sur la question de blocage administratif, qu'il a largement combattu lorsque la droite était au pouvoir, est revenu à intervalle régulier dans les débats, mais la majorité a assuré que son texte disposait de suffisamment de garanties permettant d'assurer la protection des libertés fondamentales. Il faut donc la croire sur parole.

Prochaine étape : le Sénat
Autres articles adoptés qui pourraient bien changer la donne : les articles 10 et 11, qui simplifient les procédures de perquisition policières dans le Cloud et faciliter le déchiffrement de données récupérées au cours d'une perquisition. Le texte a donc été adopté sans changement majeurs, la droite n'ayant pas réellement réussi à durcir les mesures proposées par le PS et les mesures majeures prévues par le texte sont globalement restées intactes.
Le projet de loi doit maintenant obtenir l'approbation du sénat. Pour plus de détails, le site NextInpact a couvert de très près les débats et un compte rendu des échanges est en ligne sur leur site. Armez vous néanmoins de patience, l'article dépasse allégrement les 60 000 signes, soit un texte environ 15 fois plus long que celui que vous venez de lire. Mais cette loi n'aura plus aucun secrets pour vous.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/loi-sur-le-terrorisme-l-assemblee-nationale-valide-le-blocage-administratif-des-sites-39806557.htm
Par Louis Adam | Jeudi 18 Septembre 2014

Le site internet de la région

PACA victime d’un piratage

Le site internet de la région PACA victime d’un piratage

Le site internet de la Région Provence-Alpes-Côte d’Azur (http://www.regionpaca.fr) a été victime d’un piratage informatique le mercredi 10 septembre. Après avoir été mis hors-ligne, le site est à nouveau accessible.

Les internautes ont vu s’afficher sur leur écran une page sans aucun lien avec l’Institution régionale. Le site a été rapidement mis hors ligne afin de stopper la diffusion de cette page. Les services de la Région procèdent actuellement aux analyses techniques afin de déterminer les conditions de cette attaque et travaillent au rétablissement de l’accès au site institutionnel.
La Région a également saisi la division cybercriminalité de la Police judiciaire et informé l’Agence Nationale pour la Sécurité des Systèmes d’Information. L’Institution entend porter plainte afin qu’une enquête soit menée et que des poursuites soient engagées à l’encontre des auteurs de ce piratage.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.nicematin.com/derniere-minute/le-site-internet-de-la-region-paca-victime-dun-piratage.1899236.html

---

Les Inrocks – Signaler les radars de police sur Facebook peut mener devant le tribunal

Signaler les radars de police sur Facebook peut mener devant le tribunal

Prévenir ses amis Facebook de la présence d'un radar à la sortie d'un tunnel peut vous conduire devant la justice. Le procès qui se tient ce mardi 9 septembre au tribunal correctionnel de Rodez (Aveyron) en témoigne. Quinze personnes membres du groupe Facebook "qui te dit où est la police en Aveyron" comparaissent aujourd'hui pour avoir divulgué les emplacements des radars de leur département sur le réseau social. Aux yeux du procureur de la République, elles se sont "soustraites à la constitution des infractions routières".

Des milliers de fans sur Facebook

Il n'y a bien entendu pas qu'en Aveyron que des utilisateurs de Facebook signalent à leurs "amis" les contrôles radars qu'ils constatent en temps réel. Dans les Landes, à Orléans, dans les Bouches du Rhône… Un coup d'œil sur votre smartphone, et vous évitez de vous faire flasher dans ces régions-là.


À PROPOS 10 150 membres

Groupe public

Tu es en voiture et tu vois une camionnette bleu, un radar, des motards dans l'Aveyron... viens le signaler sur ce groupe pour en informer les personnes autour de toi.
Cella ne te prendras que 30 secondes et tu seras peut être un héros pour les personnes qui vont lire ton message.

LE SEUL GROUPE UTILE !!!

Attention ce groupe est destiné à un usage informationnel et préventif, et ne nuira en aucun cas aux forces de l'ordre.
Merci de votre contribution et soyons tous solidaires ! Bonnes routes =)

Capture d'écran du groupe "qui te dit où est la police en Aveyron"

La page dédiée à l'Aveyron réunissait 10.000 fans. Selon l'avocat de neuf des prévenus, Rémy Josseaume, ce genre de groupes réunit entre 600.000 et 800.000 fans en tout. Des groupes fermés ou publics aux profils dédiés, Facebook regorge de ces pages qui vous disent qu'il y a des gendarmes au rond-point, les jumelles sur le pont ou un radar embarqué sur telle autoroute. La plupart avertissent également des travaux et des accidents. Et certains en profitent pour manifester leur mécontentement : "parce qu'il y en a marre de se faire voler des points", parmi les statuts les plus softs. Huit des prévenus de Rodez sont d'ailleurs attaqués pour "outrages" pour avoir insulté les gendarmes dans leurs commentaires.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lesinrocks.com/2014/09/09/actualite/signaler-les-radars-police-facebook-mener-devant-tribunal-11523309/

A Rodez, signaler des radars sur Facebook peut vous envoyer en correctionnelle

A Rodez, signaler des radars sur Facebook peut vous envoyer en correctionnelle

Zéro tolérance. Tel est le mot d'ordre de la justice face aux partages d'informations concernant les contrôles policiers sur les réseaux sociaux. Ainsi, 10 internautes sont convoqués par la justice le 9 septembre prochain, pour avoir publié sur une page Facebook l'emplacement de radars en Aveyron. Le « Groupe qui te dit où est la police en Aveyron » compte plus de 8000 membres, alertant les conducteurs de la localisation de contrôles routiers dans la région. Cette page Facebook est dans le viseur du procureur de Rodez, qui a cité une dizaine d'internautes à comparaître en septembre devant le tribunal correctionnel. Pour intenter cette action en justice, le magistrat se base sur l'article R413-15 du Code de la Route.
Selon celui-ci, « le fait de détenir ou de transporter un appareil, dispositif ou produit de nature ou présenté comme étant de nature à déceler la présence ou perturber le fonctionnement d'appareils, instruments ou systèmes servant à la constatation des infractions à la législation ou à la réglementation de la circulation routière ou de permettre de se soustraire à la constatation desdites infractions est puni de l'amende prévue pour les contraventions de la cinquième classe ». Les dix concernés ne disposent pas de pareil dispositif et n'ont en rien « perturbé » le bon fonctionnement des radars.
Néanmoins, l'alinéa 5 de cette article, modifié par Décret du 3 janvier 2012, précise que « les dispositions du présent article sont également applicables aux dispositifs ou produits visant à avertir ou informer de la localisation d'appareils, instruments ou systèmes servant à la constatation des infractions à la législation ou à la réglementation de la circulation routière ».

Contrôle au faciès
En d'autres termes, le fait de publier sur un réseau social la localisation des forces de l'ordre est une infraction, passible d'une amende. Si la décision du procureur est justifiée devant la loi, le procès en correctionnel est sujet à caution. En effet, cet article du Code de la Route indique que lesdites infractions sont punies « de l'amende prévue pour les contraventions de la cinquième classe ». Or les contraventions relèvent du tribunal de police et non pas du tribunal correctionnel, qui n'est pas compétent pour juger ce type d'affaires. Un point sur lequel s'appuie Me Josseaume, l'avocat de trois des prévenus, interrogé par nos confrères de 01.net, pour contester la décision du procureur.
L'avocat met également en cause l'enquête à l'origine des convocations. Sur plus de 8000 membres, seuls dix ont été ciblés. Selon Me Josseaume, il s'agit de faire un exemple, puisque rien ne justifie la convocation de ces dix personnes en particulier. Ils ne sont pas les plus prolifiques en termes de publications (un des clients de l'avocat n'aurait publié qu'un seul message sur cette page) et il semble qu'aucun n'ait jamais révélé d'informations sensibles.

Un procès qui pourrait changer la donne
Dans tous les cas, le verdict du procès (si procès il y a) devrait faire jurisprudence. En effet, cette affaire, si elle devait être portée devant les hautes instances de justice, pourrait entraîner une modification de l'article R413-15. Deux cas de figures se présentent :
Les accusés sont reconnus coupables des faits qui leur sont reprochés. Dès lors, les forces de police devront se conformer à une application stricte de l'article, à savoir verbaliser tout moyen permettant de révéler la présence de radars. Stricto sensu, cela signifie que le fait d'avoir un smartphone dans son véhicule (puisque le texte précise « de détenir ou de transporter » est passible d'une amende (c'est un cas peu probable). Enfin, les GPS signalant les radars ou les zones à risque seront interdits.
Les accusés sont reconnus non coupables. Dès lors, le fait de signaler un contrôle de police, par quelque moyen que ce soit, devient totalement légal. Ainsi, les GPS et applications de type Waze ou Coyote pourraient êtres utilisés sans aucune limitation d'ordre juridique. Mais nous n'en sommes pas encore là.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

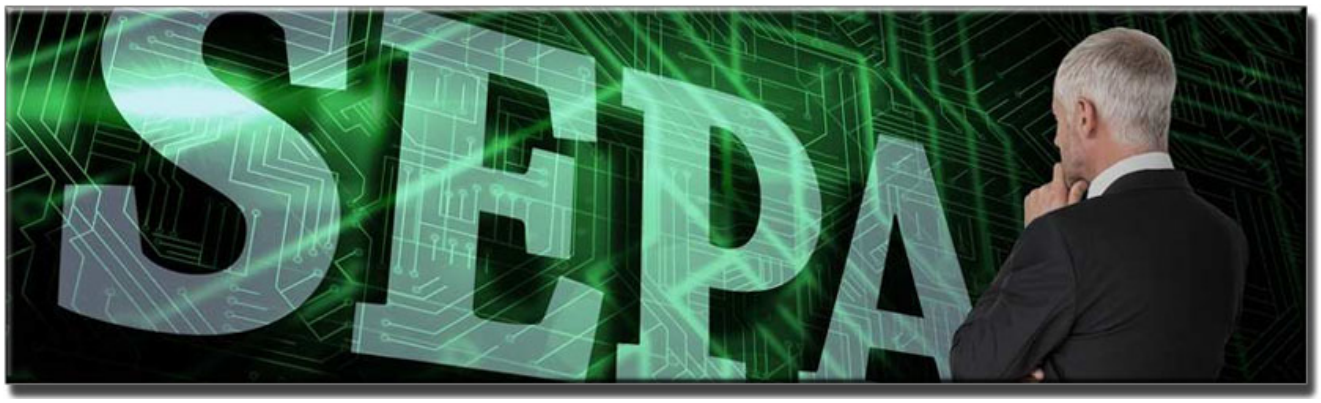
Source :
http://www.linformaticien.com/actualites/id/33405/a-rodez-signaler-des-radars-sur-facebook-peut-vous-envoyer-en-correctionnelle.aspx

Notez que pour ceux qui connaissent et qui s'intéresse à Rodez, le 4 septembre 2013, la présidente du tribunal de grande instance, Florence Peyrbène, a procédé à l'installation de deux nouveaux magistrats : Céline Gruson, nommée vice-présidente et Antoine Wolff, nommé substitut du procureur de la République.

Le 4 septembre 2013, la présidente du tribunal de grande instance de Rodez, Florence Peyrbène, a procédé à l'installation de deux nouveaux magistrats : Céline Gruson, nommée vice-présidente et Antoine Wolff, nommé substitut du procureur de la République.

Près de 20% des entreprises sont victimes d'escroqueries

bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA



Près de 20% des entreprises sont victimes d'escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA

Les entreprises font de plus en plus l'objet d'escroqueries bancaires avec un préjudice estimé à ce jour à environ 250 millions d'euros.
Les organisations professionnelles et les pouvoirs publics s'émeuvent de ce phénomène croissant qui montre l'ingéniosité de ces escrocs de plus en plus pointus en terme de détournement d'informations saisies en entrant dans les systèmes informatiques et réseaux.
Une entreprise sur six reconnait avoir été victime d'au moins une tentative de fraude en 2013. Les grandes PME sont les cibles préférées des escrocs.
Ce chiffre est le résultat d'une étude interne au secteur bancaire publié par la Fédération Bancaire Française.

Une entreprise sur deux comptant entre 500 et 1.000 salariés avec un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été visée par une tentative de fraude.

Ce chiffre descend entre 10 et 15% pour les plus petites entreprises.
Si ces fraudes touchent tous les secteurs d'activité sans exception, elles concernent plus fréquemment le commerce, compte tenu du grand nombre de transactions réalisées dans ce secteur.
Trois types de fraude à souligner :
Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, selon une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ).

1. La première d'entre elles est baptisée «escroquerie à la nigériane», en raison de l'origine des escrocs qui opèrent depuis l'Ouest africain.
Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques.
Leur méthode consiste à envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé» et …qui va donc tout droit chez eux !
2. Une autre technique de fraude est celle de l'«escroquerie au président » ou arnaque «au faux patron».
Selon le SRPJ, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG.
Ce genre d'escroquerie nécessite selon les auteurs de l'étude «une autorité naturelle, un certain aplomb et, un don pour la comédie» pour duper le comptable qui exécutera servilement les instructions écrites du « faux patron ».Ceci passe par plusieurs ruses:
La première ruse consiste à insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, ou autre évènement perturbateur annoncé.
La seconde catégorie, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes.
Cette méthode qui touche un nombre restreint d'entreprise est de loin la plus redoutable car elle émane de bandes parfaitement organisées.
Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois les plus banales, comme la fraude à la carte bancaire volée ou usurpée.
3. Enfin la dernière ruse en vigueur est celle qui profite de la norme SEPA, l'espace de paiement unique européen :Les escrocs se font passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque.
Cette technique est rendue possible par le système SEPA grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement.
Le client peut toutefois contester l'opération dans le cas où il constate un virement anormal.
60% des entreprises sont satisfaites de la réaction de leur banque.
4. Enfin, il existe aussi un dernière fraude, plus automatisée, moins humaine car basée sur le principe de fonctionnement des virus : Les ransomwares.Un ransomware, ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les modèles modernes de rançongiciels sont apparus en Russie initialement, mais on constate que le nombre d'attaques de ce type a grandement augmenté dans d'autres pays, entre autres l'Australie, l'Allemagne, les États-Unis.
Malheureusement, cette stratégie criminelle s'est avérée rentable et c'est pourquoi de nouvelles versions de cheval de Troie plus puissantes sont apparues en 2014. Nous souhaitions vous avertir contre le ransomware « Onion » (aussi connu sous le nom de CTB-Locker) qui utilise le réseau anonyme TOR (The Onion Router) et les Bitcoins pour mieux protéger des autorités, les criminels, leurs fonds et leurs clés d'accès aux fichiers des victimes.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
https://www.aiservice.fr/News/2014/Septembre/depannage-informatique-domicile-paris-2014-429-entreprises-sont-victimes-escroqueries-bancaires-derniere-ruse-norme-sepa-espace-de-paiement-unique-europeen
http://blog.kaspersky.fr/ransomwares-tor-cryptolocker/
http://fr.wikipedia.org/wiki/Ransomware
http://acteursdeleconomie.latribune.fr/finance-droit/2014-06-26/kpmg-les-dessous-d-une-escroquerie-record-a-7-6-millions.html

---

Soyez vigilants: Usurpation d'identité, « Escroquerie au Président » ou « Escroquerie au dirigeant » ça n'arrive pas qu'aux autres…

« Escroquerie au dirigeant » ou « Escroquerie au Président » ça n'arrive pas qu'aux autres…

Il me semblait important de vous informer d'un type d'utilisation des données personnelles que l'on vole aux opérateurs, entreprises, particuliers…Méthode redoutable basée sur l'usurpation d'identité, aucun système de sécurité informatique ne peut l'empêcher
Denis JACOPINI
L'Escroquerie au Président : faux dirigeants et véritable escroquerie !
L'imagination humaine étant rarement à court d'idée ; une vague d'escroqueries est en recrudescence ces derniers temps : l'« Escroquerie au Président ».

Media Participations : 987000 euros (tentative)
Areva, Scor, Quick, Nestle, CMA CGM, Michelin : Montant inconnus (Tentatives)
Elysée : 2 millions d'euros (tentative)
Valrhona : 400000 euros (tentative)
Le groupe Terrena : 489 872 euros puis 3,4 millions d'euros (tentative)
Brittany Ferries : 1 million d'euros (réussite)
Vinci : Montant non divulgué (réussite)
Robertet, l'un des leaders mondiaux des parfums implanté à Grasse : 900000 euros (réussite)
Société spécialisée dans l'optique dans le Pas-de-Calais : 497 000 euros (réussite) et 800 000 euros gelé au dernier moment par la police…
Michel (le transporteur) : 7000 euros (réussite)
KPMG : 7,6 millions d'euros (réussite)
Pour arriver à leurs fins, les aigrefins ont recours à des méthodes très pointues. Dans l'arnaque aux faux virements, ils commencent par mener une enquête fouillée sur leurs cibles. « Pendant un mois, une équipe se renseigne sur la société et ses filiales à l'étranger, témoigne Bernard Petit, sous-directeur à la lutte contre la criminalité organisée, l'un des pontes de la police. Elle collecte les PV d'assemblées générales et de conseils d'administration, et s'imprègne de la culture maison en étudiant les messages des dirigeants aux salariés ou les newsletters internes aux directeurs. » Les filous vont même jusqu'à enquêter sur la vie privée des cadres de l'entreprise. « Grâce aux réseaux sociaux, Facebook ou Twitter, ils peuvent savoir le prénom des enfants ou la date d'anniversaire de la secrétaire », relève Michèle Bruno, chef de la brigade de répression de la délinquance astucieuse.

En quelques années, les as de "l'escroquerie au Président", comme l'appellent maintenant les spécialistes, ont prélevé environ 100 millions d'euros aux sociétés françaises et à leurs banques, selon le commissaire Souvira, patron de l'Office central de lutte contre la grande délinquance financière (OCLGDF) en Janvier 2013. « Jusqu'à deux tentatives par jour enregistrées dans les grands groupes français et pas moins de 700 faits ou tentatives recensés entre 2010 et 2014.=
.Mi 2014, 250 millions d'euros ont été extorqués par ce biais aux entreprises françaises depuis 2010.

Ce type de filouterie bénéficie d'un mode opératoire très simple :
– Le fraudeur contacte, par téléphone ou par écrit, les services comptables de la société cible en se faisant passer pour son Président. Ces prises de contact ont fréquemment lieu en période de vacances, lorsque les dirigeants sont absents.
– Il invoque alors une opération confidentielle en cours (facture urgente à régler, acquisition, contrôle fiscal…) nécessitant un virement conséquent et urgent à destination d'un pays étranger.
– Devant l'urgence de la situation, la force de persuasion de l'interlocuteur (imitation de la voix, connaissance de l'organigramme de l'entreprise…) et l'intimidation dont il fait preuve (menace de licenciement) le comptable sollicité s'exécute.
Les opérations demandées sont généralement réalisés en dehors du processus habituel via une procédure de virement manuel, en raison de leur sécurisation moindre. Les sommes en jeu peuvent être considérables : entre 100.000 euros et plusieurs millions d'euros.

Afin de vous prémunir contre ce type d'escroquerie, plusieurs actions sont à réaliser en amont :
– Informer vos salariés de ces manœuvres et mettre en place un processus de sécurisation ;
– Rappeler aux services comptables et financiers de s'en tenir strictement aux procédures habituelles appliquées en matière de paiement et de signaler à la DAF toute demande inhabituelle ;
– Ré-examiner les procédures de virements manuels pour s'assurer qu'elles sont correctement sécurisées, notamment prévoir un double contrôle pour tout virement important ;
– Examiner la sécurité des accès au système d'information de l'entreprise pour vérifier son intégrité et rappeler aux salariés l'importance de ne pas livrer sur les réseaux sociaux des informations qui pourraient être utilisées aux dépens de l'entreprise…. Tels que les données personnelles des dirigeants, leurs coordonnées, leur planning, tout acte présentant la signature d'un membre de la direction, le cachet de l'entreprise …

Si vous êtes victime d'une telle escroquerie, en premier lieu :
– Portez plainte dans les plus brefs délais, même si l'escroquerie a été déjouée ! Souvent cette démarche est accompagnée d'une usurpation de l'identité du Président ou de membres de la direction ;
– Prenez contact avec un avocat spécialisé pour vous aider à mettre en place la stratégie nécessaire à la défense des intérêts de votre société mais également des intérêts des personnes physiques dont l'identité aura été usurpée.

Ce type d'escroquerie se démultiplie ces derniers temps, nous accompagnons nombre de nos clients qui sont victimes de tentative de cette nature depuis ces 24 derniers mois : Les modes opératoires de ce type de fraude varient et continueront à se perfectionner.

Il faut rester vigilant et surtout réagir très vite lorsque vous avez connaissance d'une telle fraude ou tentative de fraude.
Claudia WEBER, Avocat Associée, et Arthur DUCHESNE, Elève Avocat

---

Au travers de conférences ou de formations, Denis JACOPINI sensibilise des directeurs, des cadres et des salariés aux risques induits par les nouveaux usages de l'informatique en entreprise et dans les collectivités, ainsi que leurs responsabilités pénales.
Contactez-nous

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.itlaw.fr/fr/index.php/articles/287-l-escroquerie-au-president-faux-dirigeants-et-veritables-escroqueries
http://www.challenges.fr/entreprise/20120516.CHA6506/menace-sur-le-cac-40-les-nouveaux-escrocs-pechent-au-gros.html
http://business.lesechos.fr/directions-generales/partenaire/attention-a-l-escroquerie-au-president-4416.php
http://www.egaliteetreconciliation.fr/Alerte-sur-une-gigantesque-arnaque-israelienne-aux-faux-virements-26662.html