Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Les débordements lors des manifestations organisées chaque semaine contre le projet de loi Travail ont fait réagir Bruno Retailleau. Le sénateur LR vient de déposer une proposition de loi pour instituer notamment un nouveau fichier, celui des interdits de manifester.

Manifester paisiblement, oui, dans la violence, non. Tel est l'angle du texte déposé la semaine dernière par le parlementaire de l'opposition. Son auteur réprouve le fait que désormais, « *les forces de l'ordre sont, de façon répétée, prises pour cible à l'occasion de ces rassemblements* ». Et selon lui, « *un palier dans l'expression de la violence a été franchi, le 18 mai dernier, au cours d'une manifestation interdite lors de laquelle deux fonctionnaires de police ont été lâchement pris à partie et violemment agressés* ».

Dirigée contre les « *casseurs* », dixit son introduction, cette PPL s'inspire du mécanisme existant à l'encontre des hooligans. Le premier article veut ainsi permettre aux préfets de prononcer une mesure d'interdiction de manifester à l'encontre de toute personne « *ayant pris une part active dans un précédent attroupement en cherchant à entraver, par la force ou la violence, l'action des pouvoirs publics* » ou « *impliquée dans la commission d'un acte de dégradation ou de violence à l'occasion de l'une de ces manifestations* ». L'arrêté s'étendrait jusqu'à 12 ou 24 mois selon le comportement de la personne.

Un fichier des interdits de manifester

Pour épauler l'interdiction, qui doit être validée par un vote de l'Assemblée nationale et du Sénat, un traitement automatisé serait nourri de ces arrêtés d'interdiction, mais aussi des noms des personnes condamnées à la peine d'interdiction de participer à des manifestations sur la voie publique (L. 211-13 Code de la sécurité intérieure).

Après passage par la CNIL, sa finalité serait « *de prévenir les troubles à l'ordre public, les atteintes à la sécurité des personnes et des biens ainsi que les infractions susceptibles d'être commises à l'occasion des manifestations sur la voie publique et des rassemblements en lien avec ces manifestations se tenant dans le ressort de leur département* ».

Accentuation du périmètre de la « vidéoprotection »

Ce n'est pas tout. L'article 3 vient modifier le régime de la « vidéoprotection ». À ce jour, le Code de la sécurité intérieure autorise « la transmission et l'enregistrement d'images prises sur la voie publique » lorsqu'il s'agit d'assurer « la protection des bâtiments et installations publics et de leurs abords », « la sauvegarde des installations utiles à la défense nationale », « la constatation des infractions aux règles de la circulation », la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés, ou encore la prévention d'actes de terrorisme.

La proposition de loi aimerait ajouter au long inventaire, « *la prévention des troubles à l'ordre public en cas de manifestation sur la voie publique, au besoin au moyen de dispositifs mobiles* ». Pourquoi ? Selon le parlementaire, « *visionner la voie publique ou un lieu ouvert au public n'est possible que dans des cas et pour des motifs définis par la loi. [Cet article] rend possible la mise en œuvre d'un système de vidéo-protection sur le parcours et aux abords immédiats d'une manifestation. Afin d'assurer la faisabilité technique du dispositif, il est prévu de recourir à des caméras mobiles. L'arrêté d'autorisation déterminera la position de chacune des caméras et la période de temps au cours de laquelle le dispositif pourra être utilisé.* »

« Des objets susceptibles de constituer une arme »

La PPL s'intéresse tout autant au Code pénal, et spécialement à l'article concernant la participation délictueuse à une manifestation. Aujourd'hui, il punit de trois ans de prison de prison et 45 000 euros d'amende le fait d'y prendre part en étant porteur d'une arme.

Pour mieux assurer la préservation de l'ordre public, Bruno Retailleau y ajoute le fait « *d'introduire, de détenir ou de faire usage de fusées ou artifices de toute nature ou d'introduire sans motif légitime tous objets susceptibles de constituer une arme* » et celui « *de jeter un projectile présentant un danger pour la sécurité des personnes dans une manifestation sur la voie publique*», sachant que « la tentative de ces délits [sera] punie des mêmes peines ».

Toujours dans cette optique, elle rêve également d'instaurer une prune de 3 750 euros pour quiconque aura introduit ou consommé de l'alcool dans une manifestation sur la voie publique ou participé à une telle réunion « *en état d'ivresse* ».

Provocation à la haine contre les policiers

Outre un élargissement des possibilités d'interdire une personne à participer à des réunions et une obligation de pointage pour les personnes condamnées par un tribunal, la loi de 1881 sur la presse profite également d'une mise à jour. L'idée ? Ériger en infraction le fait de provoquer à la discrimination, à la haine ou à la violence à l'égard d'une personne « *à raison de sa profession* » (jusqu'à un an d'emprisonnement ou/et de 45 000 euros d'amende).

Pour le cas présent, la profession visée est évidemment celle des gendarmes et des policiers. Seront donc concernés ceux qui auront incité, notamment sur Internet, à la haine à l'égard des forces de l'ordre. Le dernier article prévoit d'ailleurs d'instaurer une période de sûreté pour les auteurs de violences contre elles.

S'assembler oui, mais « paisiblement »

Pour justifier son texte, Retailleau se souvient que « *l'article 7 de la Déclaration des droits de l'homme et du citoyen consacre 'le droit de s'assembler paisiblement'* ». Dans le texte fondateur, le principe est plutôt inscrit à l'article 10 (« *Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi* »).

Les adversaires d'un tel dispositif se rappelleront que la Déclaration de 1789 prévoit aussi que « *la Loi ne doit établir que des peines strictement et évidemment nécessaires* » (article 8) sachant que quiconque a le droit de résister à l'oppression (article 2) et que « *la garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée* » (article 12).

Merci à Marc Rees, auteur de cet article

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

- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE

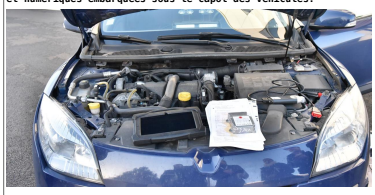
Contactez-nous

Réagissez à cet article

Source : *Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester – Next INpact*

Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact

L'Ordinateur de bord de votre voiture n'aura bientôt plus de secret pour les autorités. Une disposition adoptée dans le projet de loi sur la justice du XXIe siècle va autoriser gendarmes et policiers à fouiller les données physiques et numériques embarquées sous le capot des véhicules.



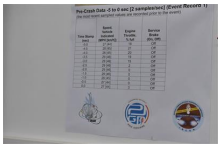
C'est un champ d'investigation suivi de près par les autorités, comme cela a pu nous être expliqué en janvier dernier, lors d'une visite au Pôle judiciaire de la Gendarmerie nationale de Cergy-Pontoise. Dans les véhicules les plus récents, les agents peuvent techniquement scruter tous les relevés techniques glanés quelques secondes avant un accident de la route. Vitesse, direction, freinage, etc. sont une mine d'informations pour confirmer ou fragiliser les affirmations du type : « *je roulais à 50 km/h, j'ai immédiatement freiné lorsque j'ai vu la future victime traverser la route* ».

Dans le projet de loi sur la justice du XXIe siècle, un amendement du gouvernement pousse davantage encore l'usage de ces investigations. Ce texte, numéroté CL180, avait été adopté en commission des lois début mai. Il a été conservé en l'état lors de la séance publique, la semaine dernière :
« *Art. L. 311-2. – Les agents compétents pour rechercher et constater les infractions au présent code, dont la liste est fixée par décret en Conseil d'État, ont accès aux informations et données physiques et numériques embarquées du véhicule afin de vérifier le respect des prescriptions fixées par le présent code* ».

L'article intègrera le titre Ier du Code de la route relatif aux dispositions techniques. Il autorisera les agents, désignés par décret, à avoir un plein accès aux données physiques et informatiques de votre véhicule. Pour cela, ils n'auront qu'à justifier de la recherche ou de la constatation d'une infraction au Code de la route. Si la pêche est bonne, alors on passera du contrôle à la possible sanction.

La cible, le diagnostic embarqué… mais pas seulement

Dans son exposé des motifs, le gouvernement souligne qu'il s'agit d'ouvrir « *notamment* » un accès « *aux systèmes de diagnostic embarqués* ». Concrètement, via un ordinateur portable connecté sur la prise de l'ordinateur de bord, policiers et gendarmes pourront prendre connaissance des données issues « *notamment* » des capteurs.



Analyses menées à Cergy-Pontoise Crédits : Marc Rees (CC BY SA 3.0)

Selon l'exécutif, la proposition a été soufflée par le comité interministériel de sécurité routière. Seulement, s'il l'envisage « *dans le cadre du contrôle du respect des dispositions techniques liées aux véhicules* », son texte est bien plus large. Le gouvernement a d'ailleurs ajouté cette phrase, à la fin de l'article : « *le fait que ces opérations révèlent des infractions autres que celles visées au premier alinéa ne constitue pas une cause de nullité des procédures incidentes* ». En clair, en recherchant des infractions au Code de la route, les agents pourront en toute quiétude découvrir d'autres éléments illicites, par exemple planqués dans un disque dur connecté au véhicule.

La latitude est d'autant plus large que n'est pas spécifié l'art et la manière dont aura lieu l'accès. Celui-ci pourra donc se faire par liaison physique (connexion par câble sur la prise du système embarquée), ou pourquoi pas à distance, avec le développement des véhicules connectés.

Le Syndicat de la magistrature réclame un encadrement de l'accès

De son côté, le Syndicat de la magistrature se dit « *hostile à l'introduction d'un [tel] article donnant accès aux informations et données physiques et numériques embarquées du véhicule sans autre condition que « pour rechercher et constater les infractions au présent code » et en permettant que les infractions révélées incidemment puissent être utilisées alors même qu'elles ne correspondent pas à celles recherchées* ». Selon le SM, une telle extension en effet, « *ne saurait être ainsi avalisée, sans aucun contrôle de nécessité ou de proportionnalité, ni procédure encadrant ces accès* ».

Adopté par les députés, mais non encore par les sénateurs, cet article va faire l'objet d'un arbitrage en Commission mixte paritaire dans les prochains jours.

Fichier des assurances, contrôles par lecture automatisé des plaques

Toujours dans le secteur de l'automobile, le même projet organise également la création d'un fichier des assurés, qui sera exploité par les dispositifs de contrôle automatisés et de vidéoverbalisation.

Un autre projet de loi, celui sur la réforme pénale a, lui, augmenté les hypothèses où les services de police, de gendarmerie nationale et des douanes pourront mettre en place une LAPI (ou Lecture automatique de plaques minéralogiques) ainsi qu'une prise photographique des occupants d'un véhicule. Ces hypothèses sont celles inscrites à l'article 706-73-1 du Code de procédure pénale, à savoir l'escroquerie en bande organisée, le travail dissimulé, le blanchiment, et même la non-justification des ressources… [Lire la suite]

Merci à Marc Rees, l'auteur de cet article

Réagissez à cet article

Source : *Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact*

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse a trouvé possiblement une solution radicale pour lutter contre la présence des téléphones portables dans les prisons : elle veut tout simplement pouvoir faire désactiver la carte SIM en cause dans les mains des opérateurs.

Les tribunaux de shérif d'Écosse (ou «Sheriff courts») auront bientôt la compétence de contraindre les opérateurs télécoms à déconnecter les téléphones portables non autorisés dont on détecterait une utilisation en prison. Concrètement, le tribunal ordonnera à l'opérateur de réseaux de désactiver ou déconnecter un téléphone mobile et/ou une carte SIM. C'est le sens d'un texte qui vient d'être notifié à Bruxelles, cette disposition imposant une restriction normative dans un État membre.

Accéder aux réseaux sociaux, intimider les témoins

« *Des détenus ont utilisé des téléphones portables non autorisés pour accéder aux réseaux sociaux, intimider des témoins et poursuivre et contrôler leurs activités criminelles depuis les institutions pénitentiaires,* expliquent les autorités écossaises en appui de leur texte. *Ils représentent par conséquent une menace notable pour la sécurité et le bon fonctionnement des établissements pénitentiaires.* »

Le hic est qu'actuellement, « *il est extrêmement difficile de trouver à l'intérieur d'institutions pénitentiaires des cartes SIM en raison de leur taille. Si c'est moins le cas pour les téléphones portables, ces détenus qui ont pris possession de téléphones portables seront prêts à faire l'impossible pour empêcher la détection desdits téléphones, notamment par des menaces et l'intimidation d'autres personnes.* »

En France, le projet de loi sur la réforme pénale

Le texte pourra entrer en vigueur dans trois mois, une fois achevé le round de la notification bruxelloise. En France, si les pouvoirs du juge profitent théoriquement d'une large latitude pour ordonner ce type de mesure, dans le projet de loi sur la réforme pénale, la réaction du législateur gagne plusieurs crans au-dessus par rapport aux textes antérieurs.

D'un, le pénitentiaire va devenir un service du renseignement. De deux, les autorités, qu'elles soient judiciaires ou administratives et sans qu'on sache très bien où se placera la frontière de leurs compétences, pourront installer une ribambelle de dispositifs techniques pour détecter des communications, et notamment des IMSI catchers. De là, elles seront en capacité d'effectuer des interceptions de sécurité pour prendre connaissance des correspondances échangées avec l'extérieur, etc… [Lire la suite]

Marc Rees auteur de cet article

Réagissez à cet article

Source : *L'Écosse veut désactiver les téléphones utilisés en prison – Next INpact*

La Cnil accorde un sursis à

Facebook pour faire preuve de loyauté (ou pas)

	La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas)

Alors qu'il s'apprête à lancer de la publicité ciblée hors de ses services, y compris auprès des non-utilisateurs de sa plateforme, Facebook a obtenu un sursis de 3 mois de la Cnil. L'autorité lui reproche une collecte déloyale de données personnelles.

Le réseau social a été mis en demeure le 9 février par l'autorité française de protection des données personnelles. La Cnil reproche à Facebook une collecte déloyale de données de navigation d'internautes non membres et l'absence de recueil d'un consentement pour le croisement de données à des fins publicitaires.
La firme de Mark Zuckerberg disposait d'un délai de trois mois pour se mettre en conformité. Mais d'après le JDN, Facebook a sollicité auprès de la Cnil un délai supplémentaire de trois mois. Celui-ci lui a été accordé.

Sécurité et publicité grâce au même cookie finalement

« Nous avons repoussé au 9 août le délai obligatoire pour se mettre en conformité » répond la Cnil. Sur le plan commercial, Facebook se montre plus dynamique. La société a annoncé tout récemment un changement de cap.
Elle entend en effet proposer de la publicité ciblée à tous les internautes et non uniquement à ceux inscrits sur son réseau. Pour suivre ces internautes,Facebook met à profit son cookie Datr. La firme assurait pourtant jusqu'à présent que ce cookie avait pour seule finalité la sécurité.
Plus d'ambiguïté à présent. Le réseau social précise que sa régie publicitaire, Audience Network, suivra dorénavant l'ensemble des internautes via ses cookies « même ceux qui ne disposent pas de compte Facebook ou ne s'y connectent pas. »… [Lire la suite]
Merci à ZdNet

Réagissez à cet article

Source : *La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas) – ZDNet*

24.000 bitcoins saisis par la police vendus aux enchères

24.000 bitcoins saisis par la police vendus aux enchères

La police Australienne va mettre aux enchères, le 20 juin 2016, 24.000 bitcoins saisis dans des affaires criminelles. Montant du lot, plus de 15.000 euros.

15 882 euros de bitcoins saisis par la justice (24,500 BTC) vont être mis aux enchères, le 20 juin, par la police australienne. De l'argent « dématérialisé » qui sera mis en vente le 20 juin 2016. Pour les autorités, cet argent « virtuel » doit être converti en monnaie sonnante et trébuchante afin de le reverser à l'autorité fiscale locale. Ces bitcoins ont été saisis dans des affaires criminelles et la police a décidé de passer par le mode enchères publique pour s'en débarrasser. C'est la société Ernst & Young qui va se charger de la vente. Ca sera la deuxième vente mondiale de ce type de « produit ».

24.000 Bitcoins saisis

Je vous révélais, en 2014, comment la police fédérale américaine des US Marshall avait revendu pour treize millions de dollars de Bitcoins (144.000 BTC), soit l'équivalent de 8.431.689 euros, dans une vente aux enchères qui commercialisait les BTC du propriétaire de Silk Road, Ross Ulbricht, une boutique du blackmarket spécialisée dans la commercialisation de drogue.
Les bitcoins australiens, ils sont au nombre de 24.518, ont été confisqués en décembre 2013 dans une affaire de drogue, à Melbourne. Son propriétaire, Richard Pollard, 32 ans, a été condamné en octobre 2015, à 11 ans de prison pour trafic de drogue… sur le site Silk Road. Les bitcoins seront vendus par lots d'environ 2.000 BTC… [Lire la suite]
Article original de Damien Bancal

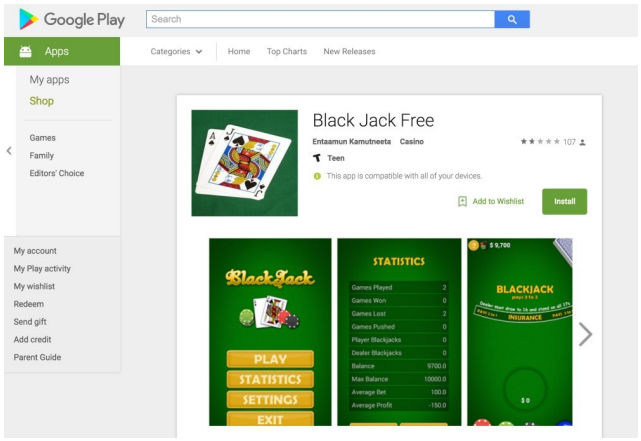
Réagissez à cet article

Source : *ZATAZ Vente aux enchères de 24.000 bitcoins saisis par la police – ZATAZ*

Alerte : Un Trojan détecté sur Google Play

Alerte : Un Trojan détecté sur Google Play

Lookout, spécialiste dans la sécurité mobile a détecté « Black Jack Free », un jeu gratuit sur Google Play qui appartient à la famille du Trojan Acecard.



S'il est de bon augure de se méfier des jeux d'argents, il faut les craindre d'autant plus lorsqu'ils sont sur internet. L'application Black Jack Free qui était en fait un Trojan a été téléchargée plus de 5000 fois avant d'être retirée du Google Play Store quatre jours plus tard. A première vue, il n'y avait rien à craindre de ce jeu de cartes qui permettait de jouer gratuitement tout en utilisant de l'argent fictif. Sauf que, dans l'arrière boutique l'application dérobait des données, mais aussi de l'argent sur les comptes en banque des utilisateurs. «Black Jack Free n'était pas directement le problème. Mais il installait une deuxième application, Play Store Update qui repérait les applications actives sur internet et imitait les pages d'accueil» explique Arnaud Simon, responsable technique Europe du sud chez Lookout.
Par ce stratagème, l'application superposait des fenêtres sur les applications bancaires, ou sur les réseaux sociaux comme Facebook ou Skype par exemple. Ensuite, les utilisateurs entraient leurs codes et identifiants sans se douter que des pirates les récupéraient. Play Store Update pouvait aussi intercepter des SMS, les envoyer vers un serveur malicieux, transférer des appels, verrouiller l'écran et effacer les données d'un terminal.

Un risque plus ou moins écarté

Il est donc fortement conseillé aux utilisateurs ayant téléchargé Black Jack Free de supprimer l'application de leurs terminaux Android et de se débarrasser de Play Store Update également. Ensuite, pour éviter les mauvaises surprises, Lookout invite les personnes concernées à modifier leurs codes d'accès.
A noter que « l'application était disponible sur Google Play car les pirates disposaient d'un accès potentiel à de nombreux terminaux. Mais les hackers ne se sont pas contentés de diffuser Black Jack Free sur cette seule et unique plateforme, elle est disponible ailleurs sur le web», ajoute Arnaud Simon. Comprendre que le Trojan court toujours et que la méfiance reste de mise.
Article original de Victor Mayet

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Un Trojan détecté sur Google Play*

Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

	Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.
Nous connaissions la Fraude au Président, l'arnaque aux faux virements via des informations bancaires soutirées à des entreprises par ruse. Un piège qui fonctionne, malheureusement aussi, sur les locataires de logements sociaux. Les escrocs se font passer pour le bailleur afin de faire modifier les données concernant les virements des loyers.
Aujourd'hui, je viens d'apprendre une nouvelle ruse. Des escrocs se font passer pour les stars de la radio (Manu de NRJ, Camille Combal de Virgin Radio…) en téléphonant et en promettant de l'argent à leurs interlocuteurs. « Un homme dans un soi-disant bureau d'antenne de radio vous dit que vous venez de gagner 2000€ et de doubler vôtre salaire, souligne l'un des témoins de ZATAZ.COM. Il y a beaucoup de bruit derrière. Comme dans un studio de radio ».

Ils visent vos informations bancaires

Une fois l'interlocuteur appâté, l'appel est transféré à une standardiste « On vous demande un numéro de compte bancaire, souligne un autre lecteur de ZATAZ. Ce qui m'a mis la puce à l'oreille est que le soi-disant animateur fusionne plusieurs jeux du 6/9 de NJR et de Virgin Radio. Pour mettre la personne en confiance, on vous ovationne et félicite pour votre prix. »
La question est de savoir maintenant comment les escrocs peuvent avoir le numéro de téléphone portable et l'identité complète (Nom, prénom) des personnes appelées.
Bref, prudence ! Si vous ne vous inscrivez pas à un jeu officiel, il n'y a pas de raison que ce dernier vous téléphone !… [Lire la suite]

Merci à Damien Bancal auteur de cet article

M

Réagissez à cet article

Source : *ZATAZ Informations bancaires : des pirates se font passer pour Manu, Camille Combal – ZATAZ*

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

Denis JACOPIN sera présent à l'IT Forum 2016 les 7 et 8 juin prochains, invité auprès des plus grands Experts en Cybersécurité. La 8ème édition de ce Forum aura pour thème Protection des Données, Gestion de l'identité numérique, Protection des transactions à l'ère du numérique : Risques, Enjeux et Stratégies de mise en oeuvre.

2 jours de networking organisés par CIO Mag et le Club DSI de côte d'Ivoire sous le parrainage de

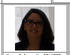
Bruno Nabagné KONE,
Ministre de l'Economie numérique et de la Poste – Côte d'Ivoire

Venez discuter, échanger et dialoguer avec des donneurs d'ordre, rencontrez-les en rendez-vous :


Freddy TCHALA, CEO MTN CI


Euloge SORO-KIPEYA, CEO ANSUT


Nongolougo SORO, CEO SNDI


Mme. Saloua K. BELKZIZ, Présidente de la Fédération APEBI – Maroc


Jean Kacou DIAGOU, Président du CGECI – Côte d'Ivoire

Une vingtaine d'experts partageant leurs retours d'expériences et les meilleures pratiques


Cdt Guelpétchin Ouattara, Directeur de l'Informatique et des Traces Technologiques – Côte d'Ivoire


Yann PILPRE, Expert Sécurité, CEO YPSI


Denis JACOPINI, Expert en Cybercriminalité et Protection des données personnelles


Ange DIAGOU, CEO NSIA Technologies


Frédéric MASSE, Vice-Président SAP


Alain DOLIUM, Expert Transformation numérique PDG SMS Group

vous souhaitez y participer ?
Entrée gratuite mais inscription obligatoire : Cliquez ici

PROGRAMME

Heures	Activités	Intervenants
Journée du Mardi 07 juin 2016		
08h00 – 09h00	Accueil et installation des invités	*Comité d'organisation*
09h00 – 09h05	Mot de Bienvenue	· **M. Mamadou NAON,** Président CDSI
09h05 – 09h15	Mot du Sponsor Officiel	· **M. Freddy TCHALA,** DG MTN
09h15 – 09h25	Mots des sponsors Leaders	· **M. Nongologou SORO,** DG SNDI · **M. Ange DIAGOU,** DG NSIA TECHNOLOGIES
09h25 – 09h35	Présentation du contenu de l'IT FORUM 2016	· **M. Mohamadou DIALLO**, Directeur de Publication CIO MAG
09h35 – 09h40	Mot du Pays Invité (Maroc)	· **Mme Saloua K. BELKZIZ**, Présidente de la Fédération APEBI
09h40 – 09h50	Mot du Président de l'IT FORUM 2016	· **M. Jean Kacou DIAGOU,** Président CGECI
09h50 – 10h05	Discours d'ouverture des travaux	· **M. Bruno KONE,** Ministre de la Poste et de l'Economie Numérique
10h05 – 10h20	REMISE DE TROPHEES	
10h20 – 10h45	Coupure de ruban – Visite des stands – Cocktail	
10h45 – 10h50	**TIRAGE TOMBOLA**	
10h50 – 11h05	Les principales tendances IT en Afrique occidentale et centrale	· **M. Mohamed ZIZI,** Directeur régional pour l'Afrique Francophone IDC
11h05 – 12h00	Plénière/Panel 01 **La protection des données, une nécessité pour le respect des libertés fondamentales**	· **Cdt Guelpétchin Ouattara**, Directeur de l'Informatique et des Traces Technologiques (DITT Côte d'Ivoire) · ***Ibrahima DIAGNE,*** *Administrateur Délégué Gaindé 2000* ***Modérateur : Dr GUIBESSONGUI N'Datien Sévérin****, ICT CONSULTING* ***Rapporteur : M. Auger SEOULOU,*** *DSI Ministère de la Justice – Côte d'Ivoire*
12h00 – 12h05	**TIRAGE TOMBOLA**	
12h05 – 12H35	Atelier 01 **Optimisation des coûts en relation avec votre business model**	· **M. Christophe Thénégal,** Associé PWC
12h35 – 12h40	**TIRAGE TOMBOLA**	
12h40 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 15h20	Plénière/Panel 02 **Fluidité des transactions : Comment mieux réglementer le secteur en vue de développer l'adoption de la monnaie électronique**	· ***M. Frédéric MASSE,*** *Vice-Président SAP* · ***M. Francis Dufay,*** *Directeur Général de JUMIA Côte d'Ivoire* · ***Représentant MTN MFS*** ***Modérateur : M. Lacina KONE,*** *Conseiller NTIC –Président de la République* ***Rapporteur : M. Eric YAO****, DSI CNCE*
15h20 – 15h30	**FIGHT 1 : Logiciel open source VS Logiciel Propriétaire (compétions des solutions IT)**	
15h30 – 15h35	**TIRAGE TOMBOLA**	
15h35 – 15h50	Atelier 01	· *SAP*
15h50 – 15h55	**TIRAGE TOMBOLA**	
15h55 – 16h10	Plénière **Méthode, technique et outils des transactions électroniques et leur sécurité**	· **M. Yann PILPRE,** Expert Sécurité, DG de YPSI
16h10 – 16h20	**FIGHT 2 : Approche de sécurisation de données à caractère personnel et des transactions électroniques : méthode et outils (compétition des approches IT)**	
16h20 – 17h05	Panel 03 **Données dans le Cloud public/privé: Comment et avec qui assurer la sécurité ?**	· ***M. Nongolougo SORO,*** *DG de la SNDI* · ***M. Euloge SORO,*** *DG de l'ANSUT* · ***AUSIM*** *(Maroc)* · ***M. Brice DEMONGE,*** *Directeur de développement secteur public – GFI Informatique* · ***Camille AMEYAO / MTN Business*** · ***Denis JACOPINI,*** *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Modérateur : Conrad GBAGUIDI,*** *DG MGT Conseils* ***Rapporteur : M. Aboadjé KOUADIO,*** *DSI SNDI*
17h05– 17h10	**TIRAGE TOMBOLA**	
Fin de la première journée		

Journée du Mercredi 08 juin 2015		
08h30 – 09h15	Accueil et installation des invités	Comité d'organisation
09h15 – 09h30	Rappel des travaux de la journée du 07 juin	Club DSI
09h30 – 09h35	**TIRAGE TOMBOLA**	
09h35– 10h20	Panel 04 **Les entreprises et administrations ivoiriennes face à la cybersécurité** **–**	· **M. Freddy TCHALA**, DG MTN Côte d'Ivoire · ***M. Nongolougo SORO,*** *DG de la SNDI* · ***M.Ange DIAGOU,*** *DG NSIA Tech* · ***M. Bilé DIEMELEOU,*** *DG ARTCI* ***Modérateur : Patrick M'BENGUE, Président GOTIC***
10h20 – 10h25	**TIRAGE TOMBOLA**	
10h25 –10h40		
10h40 – 10h45	**TIRAGE TOMBOLA**	
10h45– 11h00	Atelier 04 **Les services managés: garants d'une transformation numérique efficace, rentable et sécurisée**	*NSIA TECHNOLOGIES*
11h00 – 11h15	Atelier 05	*FEITAN France*
11h15 – 11h20	**Cloud privé VS Cloud Public (Compétition des technologies Cloud)**	
11h20 – 12h15	**Comment sécuriser ses infrastructures et plateformes de services pour la transformation numérique?**	· ***Représentant de l'ARTCI*** · ***Denis JACOPINI,*** *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Jean-François TESSERAUD,*** *Chief Information Security Officer – Systemis* · ***Yves MIEZAN EZO, Conseil,*** *Stratégie & Formation Open Source* · ***Modérateur : Ludovic MORINIERE,*** *International Development BearinPoint*
12h15 – 12h20	**TIRAGE TOMBOLA**	
12h30 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 14h50	Atelier 06	VEONE
14h50 – 15h00	**FIGHT 04**	
15h00 – 15h15	Atelier 07 **Pourquoi et Comment protéger efficacement vos données dans la transformation numérique ?**	· ***Marcial MONTHE,*** *Ingénieur Avant-Vente, Responsable de la Business Unit Veritas –* ***SOCITECH***
15h15 – 15h20	**TIRAGE TOMBOLA**	
15h20 – 15h35		
15h35 – 16h40	**TIRAGE TOMBOLA**	
15h40 – 15h55	Récompense des Sponsors et Partenaires	***Club DSI***
15h55– 16h20	Restitution des travaux	
Fin de la 2ème journée		
Soirée de Gala		

Merci à l'auteur de cet article

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE – Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Jour J-16*

La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

	La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

Les attaques visant les systèmes bancaires connectés au réseau Swift soulèvent de vastes inquiétudes au point que les autorités européennes pourraient être appelées à conduire un stress-test visant à éprouver leur cybersécurité.

Recommander les autorités locales des pays membres de l'Union européenne à soumettre les systèmes de sécurité informatique des institutions financières à des stress-tests. C'est l'idée qu'a avancé Andrea Enria, président de l'Autorité Bancaire Européenne, l'autorité indépendante chargée de garantir un niveau de surveillance prudentiel efficace et cohérent à l'échelle de l'Union, à l'occasion d'un échange avec nos confrères de Reuters.
Dans ce cadre, il estime que les banques pourraient avoir à provisionner des réserves supplémentaires afin de se protéger, financièrement, du risque associé à des attaques informatiques. Le risque informatique doit d'ailleurs être explicitement pris en compte dans le cadre des règles Pilier 2. Celles-ci font partie des accords Bâle II et portent justement sur la surveillance prudentielle ainsi que la gestion des risques.
Et la prise en compte des risques associés aux attaques informatiques apparaît particulièrement importante qu'ils sont appelés à être de plus en plus considérés dans les analyses de solvabilité des agences de notation. Moody's et Standard & Poor l'ont ainsi ouvertement indiqué à l'automne dernier.
Fin 2013, les banques britanniques ont été soumises à un stress-test IT, après un premier en 2011. Mais l'opération n'avait pas manqué de soulever plusieurs critiques, certains experts estimant notamment qu'elle devrait survenir plus régulièrement. D'autres s'interrogeaient sur la manière dont étaient définies les attaques imaginées pour l'exercice.
Très récemment, la patronne du gendarme des marché boursiers américains a de son côté estimé que le risque d'attaque informatique constitue la principale menace pour le système financier mondial, notamment après les opérations qui ont visé dernièrement les systèmes plusieurs banques connectés au réseau Swift… [Lire la suite]

Merci à Valery Marchive pour son article

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Vers un stress-test de la cybersécurité des banques*

européennes ?

ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ

	**Fuites de données de Santé en France**

Santé et fuite de données – Plus de 200 millions de dossiers médicaux de ressortissants américains ont disparu depuis 2015. Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Le Parlement européen a adopté le jeudi 14 avril 2016 le règlement européen sur la protection des données. Le règlement qui sera applicable à partir du 25 mai 2018 dans l'ensemble des pays membres de l'Union européenne. Avec cette jolie annonce que l'on attend depuis des années, je me suis penché sur un cas concret de fuites de données : les dossiers médicaux. A la fin de ma compilation et analyses des datas collectées, ma question est la suivante : Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Santé et fuite de données : Plus de 200 millions de dossiers médicaux perdus en 1 an

J'ai analysé les établissements de santé américains. Il faut dire que cela est plus simple. La France n'a aucun moyen de contrôle au sujet des fuites d'informations dans le secteur Français de la santé. Et ce n'est pas faute d'avoir des personnes très compétentes au Ministère de la Santé et des Affaires Sociales. Mais en France, pour le moment, aucune obligation n'est faite pour que les patients soient alertés en cas de fuite, de piratage, de perte de leurs données (clé usb, portable…). Sur le sol de l'Oncle Sam, il en est tout autre. La loi ***Hitech Act*** *(section 13402) impose l'affichage public de toutes fuites d'informations concernant plus de 500 patients dans le même établissement.*

En 1 an, la plus grosse fuite de données médicales aux USA aura visé l'Anthem, Inc. Affiliated Covered Entity. Nous sommons alors en mars 2015. 78,8 millions de dossiers suite à un « ***Hacking/IT Incident Network Server*** *» comme le référence le Ministère américain de la Santé (****HHS****). Depuis le 1er janvier 2016, 103 établissements de santé (Hôpitaux, centres de soin…) ont été touchés par une perte, un vol, un piratage. Dernier cas en date, 2.213.597 de données de patients piratés au 21st Century Oncology de Floride. Ici aussi, le HHS (U.S. Department of Health and Human Services) parle de «* ***Hacking/IT Incident Network Server****« . L'attaque date du 4 avril 2016.*

Depuis le 1er janvier 2016, 3.605.511 dossiers de patients américains ont volés, piratés ou perdus. Et en France ?

Article de Damien BANCAL

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Santé et fuite de données : et s’il était déjà trop tard – ZATAZ*