

Google déclare la guerre à Daech

	Google déclare la guerre à Daech
---	---

Le moteur de recherche vient d'annoncer la mise en place de nouveaux moyens pour lutter contre la radicalisation en ligne. Facebook et Twitter collaborent.



Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet. Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet.

La cyberguerre est déclarée. Engagée après les attentats de Paris par les très mystérieux hackers d'Anonymous, elle est aujourd'hui rejointe par Google. Lors d'une réunion avec le comité des affaires intérieures britanniques, Anthony House, un cadre de l'entreprise de Mountain View, a exposé les plans mis en place pour lutter contre la propagande djihadiste, rapporte The Telegraph . Le géant du Web prévoit de rediriger les recherches « pro-Daech » vers des sites luttant contre la radicalisation. En effet, parmi les recrues de l'État islamique, nombreuses sont celles qui ont été endoctrinées derrière leur écran.

Mais, si l'offensive semble nouvelle, les géants d'Internet n'en sont pas à leur coup d'essai. En 2014, Google avait déjà fait retirer 14 millions de vidéos, dont certaines pour propagande, de sa plateforme YouTube.

Selon Yahoo News, Facebook a pour sa part développé au moins cinq cellules dédiées à la lutte contre le terrorisme et suit au plus près les profils signalés. Enfin, le réseau social travaille en collaboration étroite avec des imams, pour aider à la déradicalisation.

De son côté, Twitter déclare avoir supprimé plus de 10 000 comptes ouvertement djihadistes. Nick Pickles, chargé de la politique publique du site de microblogging en Grande-Bretagne, a annoncé : « Twitter, qui a 320 millions d'utilisateurs, emploie plus de 100 personnes pour s'occuper du contenu inapproprié. » Dans cette cyberbataille, Anonymous vient de trouver des alliés de taille. ... [Lire la suite]



Réagissez à cet article

Source : *Google déclare la guerre à Daech*

Comment analyser votre e-réputation sur Internet en un instant ?



Comment analyser
votre e-réputation
sur Internet en un
instant ?

Nothing to Hide devrait intéresser certains d'entre vous et c'est tout à fait normal car ce service va vous permettre d'analyser votre e-réputation en quelques secondes. Grâce à lui, vous saurez donc si tous les contenus partagés sur vos profils sociaux pourront un jour se retourner contre vous. Plutôt pratique, non ?

Les internautes sont de plus en plus actifs sur les réseaux sociaux et certains d'entre eux n'hésitent pas à partager toute leur vie sur Twitter, Facebook ou même Instagram.



Le moment est peut-être venu de commencer à soigner votre e-réputation.

Le problème, c'est que la plupart de ces données sont rendues publiques. Il suffit donc d'une requête bien sentie sur un de ces services pour trouver les photos et les publications de n'importe quel utilisateur.

Avez-vous confiance en votre e-réputation ?

La question qui se pose, c'est évidemment de savoir si votre futur patron appréciera de vous voir poser à poil devant l'objectif avec votre cousin Bébert sur les plages nudistes de la Baule, ou s'il appréciera le petit coup de gueule que vous aviez poussé en novembre 2013 contre « ces salauds de patrons qui vous sucent jusqu'à la moelle ».

Dans ce contexte, il est tout à fait primordial de soigner son e-réputation et Nothing to Hide va justement vous permettre de prendre un peu de recul sur tout ce que vous publiez à longueur de temps sur vos profils sociaux.

Le service va ainsi commencer par vous demander de vous connecter à vos comptes Twitter, Facebook, LinkedIn et Instagram.

Lorsque ce sera fait, il vous posera une vingtaine de questions personnalisées en fonction des contenus publiés sur cette plateforme et il vous demandera notamment si vous assumez telle ou telle photo ou si vous êtes toujours d'accord avec cette vieille publication que vous aviez (forcément) oubliée.

La procédure dure quelques minutes à peine

La procédure dure quelques minutes. Ensuite, le service vous affichera un score variant en fonction de vos données et de vos réponses.

Il vous permettra de savoir si vous assumez réellement vos publications et si votre réputation numérique se porte bien.

Mieux, Nothing to Hide va aussi vous attribuer un grade et il affichera en plus quelques alertes dans la foulée. Elles ne sont pas toutes très pertinentes en revanche. Tenez, par exemple, le service me reproche de ne pas connaître tous mes followers sur Instagram par exemple.

Ceci étant, il devrait tout de même être utile à certains d'entre vous, et surtout à ceux qui sont en recherche d'emploi.

Oui, car les recruteurs trainent aussi beaucoup sur les réseaux sociaux...

Nothing to Hide
BY MAZARS

LANCER LE SCAN →

Découvrir Mazars

FRÉDÉRIC PEREIRA

Votre Role :

EXPERT

Votre métier n'est bien maîtriser votre e-réputation. Choisissez bien !

75%

Votre Score

75% de réponses correctes

VOUS FAITES PARTIE DES 40,42% PERSONNES LES MEILLEURS NOTRÉS

POSTAGES

Envoyer par Mail

Vous ne connaissez pas "3" la/les personne(s) qui vous suit/vent. N'acceptez que des personnes que vous connaissez.

Valider Mon Répon.

Vous ne connaissez pas "3" la/les personne(s) qui vous suit/vent. N'acceptez que des personnes que vous connaissez.

Valider Mon Répon.

Vous ne connaissez pas "3" la/les personne(s) qui vous suit/vent. N'acceptez que des personnes que vous connaissez.

Valider Mon Répon.

Nothing to Hide
BY MAZARS

LANCER LE SCAN →

Découvrir Mazars

1. CONNECTEZ-VOUS
via les réseaux sociaux

2. RÉPONDEZ
à toutes questions

3. DÉCOUVREZ
votre profil e-réputation

20 questions maximum vous seront posées pour moins de 5 minutes.

Très belle photo ! Êtes-vous conscient(e) que tout le monde peut la voir ?

NON, PAS VRAIMENT

OUI, TOUT À FAIT !

VOUS DONNÉES NE SONT PAS UTILISÉES À DES FINS COMMERCIALES ELLES SONT UNIQUEMENT UTILISÉES POUR VOUS DONNER DES RÉSULTATS PERTINENTES.

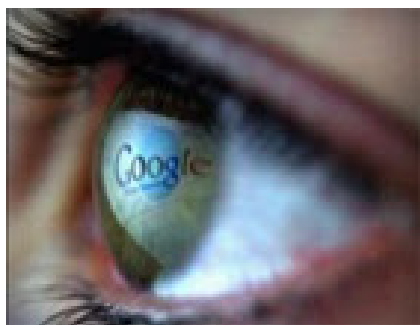
NOTHING TO HIDE by Mazars - COPYRIGHT 2016 - Mentions légales-Voir la charte

... [Lire la suite]

Réagissez à cet article

Source : Avec *Nothing to Hide*, vous allez pouvoir analyser votre e-réputation en un instant

Un casque de réalité virtuelle totalement autonome signé Google



Un casque de
réalité virtuelle
totalement
autonome
signé
Google

Alors que la rumeur initiale prêtait à Google l'intention de développer un casque de réalité virtuelle fonctionnant avec un smartphone, le Wall Street Journal affirme qu'il s'agirait en fait d'un appareil totalement autonome.

Google travaillerait sur un casque de réalité virtuelle tout en un, capable de fonctionner sans être connecté à un smartphone, un ordinateur ou une console de jeu. C'est ce qu'affirme le Wall Street Journal qui ajoute que la firme de Mountain View compte sortir cette année une évolution de son Carboard, le casque en carton qui s'adapte sur des smartphones.

Il s'agirait cette fois d'une version en plastique qui intégrerait des capteurs et un processeur. En début de semaine, le Financial Times avait fait allusion à ce second modèle, mais n'avait pas évoqué de casque tout en un.

Selon les informations du Wall Street Journal, le modèle autonome sur lequel planche Google serait équipé d'un processeur haute performance développé par Movidius, l'entreprise qui lui fournit déjà les puces pour ses terminaux du Projet Tango. Il incorporerait aussi des caméras frontales pour suivre les mouvements de tête de l'utilisateur. La date de lancement de ce casque ne serait pas encore très claire. En revanche, le modèle en plastique pourrait être dévoilé ... [Lire la suite]



Réagissez à cet article

Source : *Google développerait un casque de réalité virtuelle totalement autonome*

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données



La Commission Nationale de l'Informatique et des Libertés a publiquement mis en demeure Facebook de ne plus placer de cookies indésirables sur les postes des utilisateurs et d'arrêter le transfert des données personnelles de ses membres vers les Etats-Unis.

Le géant des réseaux sociaux a 3 mois pour se conformer à cette décision sous peine de sanction. La Commission Nationale de l'Informatique et des Libertés (CNIL) a ordonné à Facebook de stopper le transfert de certaines données personnelles de ses utilisateurs vers les Etats-Unis et de changer la façon dont elle récolte leurs données lorsqu'ils visitent son site web.

Dans sa mise en demeure, rendue publique lundi en fin de journée, la CNIL reproche ainsi à Facebook de transférer les données de ses membres aux Etats-Unis sur la base du Safe Harbor « ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne du 6 octobre 2015 », rappelle la commission.

La liste des griefs ne s'arrête pas là : « Le site dépose sur l'ordinateur des internautes des cookies à finalité publicitaire, sans les en avoir au préalable correctement informés ni avoir recueilli leur consentement », indique la CNIL.

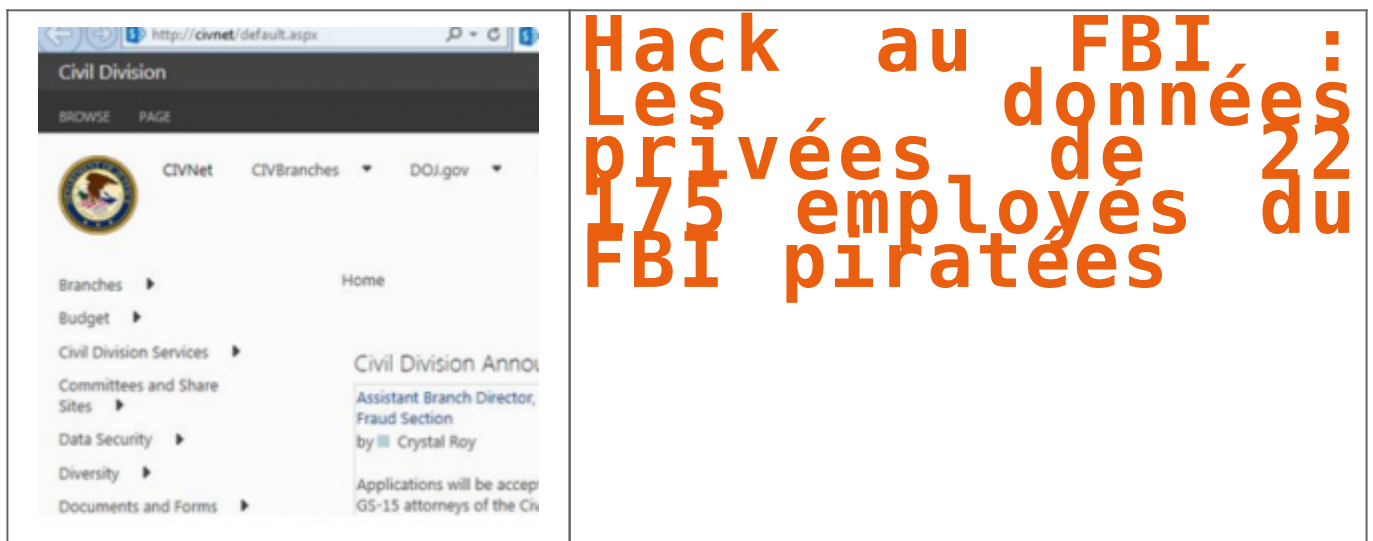
Autre constat et non des moindres : « La CNIL a constaté que le site Facebook est en mesure de suivre la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte Facebook. En effet, le site dépose un cookie sur le terminal de chaque internaute qui visite une page Facebook publique, sans l'en informer. »... [Lire la suite]



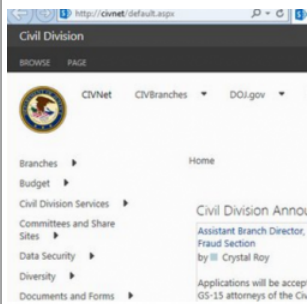
Réagissez à cet article

Source : *La CNIL lance un ultimatum à Facebook au sujet des*

Hack au FBI : Les données privées de 22 175 employés du FBI piratées



Un hacker est parvenu à s'introduire sur l'intranet du ministère américain de la Justice et à télécharger 200 Go de fichiers incluant des noms, numéros de téléphones et mails de 22 175 employés du FBI mais également des données personnelles relatives à 9 372 personnes travaillant pour le ministère de la Sûreté Intérieure des Etats-Unis.



Hack au FBI. Ce n'est malheureusement pas le nom d'une nouvelle série, mais bel et bien d'un second incident de sécurité majeur qui a permis de divulguer plusieurs dizaines de milliers de données personnelles d'employés du FBI mais également du ministère de la Sûreté Intérieure (Departement of Homeland Security). Si dans le précédent épisode du Hack of FBI en novembre dernier 3 000 coordonnées de policiers et de militaires américains s'étaient retrouvés dans la nature, le volume est donc cette fois-ci beaucoup plus important. Ainsi, le hacker, opérant sous le pseudonyme DotGovs sur Twitter, a publié une liste de 22 175 employés travaillant au FBI – parmi lesquels des agents spéciaux, analystes et officiers – incluant leurs noms, prénoms, fonctions mais également numéros de téléphone ainsi que leurs adresses mails. D'après Motherboard, qui s'est entretenu avec le hacker, ce dernier a également en sa possession des données personnelles appartenant à 9 372 employés de la Sûreté Intérieure américaine. Des données qui ont été également mises en ligne en tout début de semaine.

Alors que pour le précédent hack de données personnelles des employés du FBI, le groupe de hackers Crackas With Attitude s'en était pris au compte mail AOL du patron de l'agence, Mark Giuliano, le vol de données opéré par le mystérieux DotGovs a été effectué d'une toute autre manière. Ainsi, ce dernier a réalisé son méfait en piratant un compte mail d'un employé du département américain de la Justice. Le hacker a ensuite contacté le support du ministère en indiquant ne pas pouvoir se connecter au portail web. « Alors je les ai appelés et leur ai dit que j'étais nouveau et leur ai demandé comment accéder au portail », a expliqué le hacker à Motherboard. « Ils m'ont demandé si j'avais un code token, j'ai dit non, ils m'ont dit que ça allait et d'utiliser le leur. » Une fois connecté, le hacker raconte alors avoir cliqué sur un lien l'ayant amené sur une machine virtuelle en ligne et entré les identifiants du compte mail déjà hacké. « J'ai cliqué dessus et ai eu un accès total à l'ordinateur », a expliqué le pirate.

Un détournement classique

« Ces comptes détournés peuvent uniquement être détectés grâce à la capacité d'observer et de détecter les changements dans le comportement de l'utilisateur, par exemple la connexion de l'utilisateur à son compte à un horaire inhabituel ou d'un endroit inhabituel, la vitesse de frappe sur son clavier ou d'exécution des commandes, etc. C'est ce que l'on appelle, l'analyse comportementale des utilisateurs. Cette technologie permet de fournir un profil réel de chaque utilisateur, basé sur des caractéristiques personnelles – en quelque sorte sorte une empreinte digitale – et ainsi de détecter tout comportement anormal du compte utilisateur et d'en référer instantanément à l'équipe de sécurité voire même de bloquer en temps réel l'activité de l'utilisateur jusqu'à nouvel ordre », a par ailleurs précisé dans un communiqué Zoltán Györkö, PDG de l'éditeur en sécurité Balabit.

En tout, ce sont près de 200 Go de données confidentielles qui ont été téléchargées, alors que le hacker indique avoir eu accès à 1 To de données. « J'ai eu accès à ces données mais n'ai pas pu tout prendre », fait savoir DotGovs. Parmi les contenus qui sont passés entre ses mains ou ses yeux, on trouverait aussi des mails de militaires ainsi que des numéros de cartes bancaires. Suite à la parution de ces listes hackées de plus de 30 000 employés, le DHS a réagi par le biais de son porte-parole S.Y. Lee : « Nous recherchons les articles relatant les informations de contacts des employés du département de la sûreté intérieure qui ont été divulgués. Nous prenons très au sérieux ces articles, cependant rien ne permet d'indiquer à ce jour qu'il y ait eu violation d'informations sensibles ou personnelles. » ... [Lire la suite]



Réagissez à cet article

Source : *Les données privées de 22 175 employés du FBI piratées – Le Monde Informatique*

Toutes les versions de Windows touchées par une faille critique



Toutes les versions de Windows touchées par une faille critique

Toutes les versions de Windows, dont Windows 10, sont affectées par une faille critique pour laquelle un correctif est disponible. La vulnérabilité permet d'exécuter arbitrairement du code.

Le dernier Patch Tuesday de Microsoft est léger en correctifs critiques, mais une faille majeure cependant affecte l'ensemble des versions supportées de Windows.

Dans son bulletin de sécurité mensuel, Microsoft informe les utilisateurs de la nécessité de patcher immédiatement une vulnérabilité sérieuse au niveau de la façon dont le système d'exploitation gère certains fichiers. Toutes les versions de Windows sous support sont concernées, de Windows Vista à Windows 10.

La faille (MS16-013) pourrait permettre à un attaquant d'exécuter arbitrairement du code comme l'utilisateur authentifié sur la session Windows. Les risques sont donc accrus pour les utilisateurs avec un compte doté des droits administrateur.

Autres vulnérabilités dans Office, IE et Edge



Pour réaliser l'attaque, le pirate doit amener l'utilisateur à ouvrir un fichier Journal spécialement forgé. Il pourra ainsi exécuter des programmes, supprimer des données et même créer de nouveaux comptes avec tous les droits sur le poste Windows.

Windows Server 2016 Tech Preview 4 est également affecté par la vulnérabilité et le correctif doit donc aussi être déployé sur ces configurations. Microsoft précise toutefois n'avoir à ce jour détecté aucune exploitation de cette faille Windows.

A noter que l'éditeur a publié trois autres correctifs pour des vulnérabilités critiques de Windows et Office.

MS16-012 corrige une faille permettant à un attaquant d'exécuter du code en exploitant un fichier PDF compromis. Les utilisateurs de Windows 8.1 et Windows 10 sont principalement touchés. Le problème de sécurité a été signalé à l'éditeur par un tiers et ne ferait pas l'objet d'attaques.

MS16-015 remédie à plusieurs failles de corruption mémoire dans Microsoft Office. Elles autorisent des attaques par le biais de fichiers Office malveillants. Leur exploitation permet d'obtenir des droits équivalents à ceux de l'utilisateur de la session ouverte.

MS16-022 corrige enfin de nombreuses vulnérabilités d'Adobe Flash Player dans Windows 8.1 et versions suivantes de l'OS Microsoft.

L'éditeur diffuse par ailleurs un patch cumulatif pour Internet Explorer (MS16-009) et le nouveau navigateur de Windows 10, Microsoft Edge (MS16-011). Les différentes failles ne feraient l'objet d'aucune exploitation avant la diffusion des correctifs, toujours selon la firme de Redmond... [Lire la suite]



Réagissez à cet article

Source : Toutes les versions de Windows touchées par une faille critique

Programme de la 6eme Edition IT Forum à Dakar au Senegal Replay-

	Programme de la 6eme Edition IT Forum à Dakar au Senegal
---	---



PROGRAMME DU JEUDI 18 FEVRIER 2015

9h00-9h10 DISCOURS DE BIENVENUE

Par M. Mohamadou DIALLO, Directeur de la publication de Cio Mag

9h10-9h20 ALLOCUTION D'OUVERTURE

Approche nationale et régionale en matière de Cybercriminalité

Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications

9h20-9h30 ALLOCUTION Pays Invité d'honneur

Lutte contre la cybercriminalité, la Côte d'Ivoire renforce son arsenal

Par M. Bruno N. KONE, Ministre de la Postes et des Technologies de la Communication de Côte d'Ivoire, Porte-parole du Gouvernement

9h30-9h50 KEYNOTE SPEAKER

Pas d'Economie Numérique sans cyber-sécurité : Comment faire face aux tendances du numérique tout en maîtrisant les défis du Cyberspace ?

Par M. Thierry BRETON, Président Directeur Général d'ATOS

9h50-10h00 KEYNOTE SPEAKER

L'Arrivée des réseaux haut débit, un accélérateur ou un moyen efficace de lutter contre les cyberattaques

Session Introductive

9h50-10h30 2 POINTS DE VUE

– Cyber sécurité et protection des données à caractère personnel

Par M. Mouhamadou LO, Président de la Commission de Protection des Données Personnelles (CPD) du Sénégal

– Cybercriminalité : un enjeu international

Par M. Ali Drissa BADIOEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest

Questions / Réponses

10h30-11h00 Pause café et visite des stands

11h00-12h00 Plénière 1

Cloud, Mobilité, big data, internet des objets, Byod : Comment intégrer les nouvelles tendances tout en maîtrisant les nouveaux risques inhérents ?

Moderateur: Commandant Guelpechetchin QUATTARA, Directeur de l'informatique et des Traces Technologiques de Côte d'Ivoire

– Représentant opérateur (Orange/Figo ou Espresso Télécom)

– M. Chris MORET, Responsable de la Global Business Line CyberSecurity d'Atos Big Data & Secrity

– Dr. Alloune DIONE, Directeur des Systèmes d'Information de la Douane

– Colonel Julien DECHANET, Officier Cyber des Eléments français en Afrique de l'Ouest

– M. Jean-Paul PINTÉ, Expert International en Cybercriminalité,

– Alain DOLLIUM, Co-fondateur et CEO EMEA North America de South Mobile Service,

Questions / Réponses

12h00-13h00 Plénière 2

Plan Numérique et Administration électronique : Quelles perspectives ?

Moderateur : M. Alain DUCASS, Expert en Transformation Digitale

– Présentation des grandes lignes du Plan stratégique pour le numérique (Côte d'Ivoire/Sénégal) Par M Euloge Kipeya SORO, Directeur Général de l'Agence Nationale du Service Universel des Télécommunications (ANSUT)

– M. Malick NDIAYE Directeur de Cabinet du Ministère des Poste et des Télécommunications du Sénégal

– M. Mouhamad Tidiane Seck, Directeur Associé Performances Management Consulting

– M. Cheikh BAKHOM, Directeur Général de l'Agence de l'Informatique de l'Etat (ADIE)

– M. Brice DEMOGÉ, Directeur du développement Secteur Public et Afrique – GFI Informatique

Questions / Réponses

13h00-14h00

Pause Déjeuner

14h00-15h00 Plénière 3

Retours d'expériences : solutions

– Plan de Sauvegarde et réplication des donnée après un incidents

– SAP s'engage pour la préservation du Parc Niokolokoba

– Cloud, l'essentiel pour les entreprises

Par Opérateur (Orange/Figo ou Espresso Télécom)

– Applications métiers en mode Cloud, GFI informatique / Cegid

– Big data et sécurité, M. Alain DOLLIUM, CEO South Mobile Services

Questions / Réponses

15h00-16h00 Plénière 4

Quelles solutions face à l'internationalisation de la cybercriminalité ?

– Moderateur : M. Pape Assane TOURE, Magistrat, Secrétaire général adjoint du Gouvernement

– M. Pape GUEYE, Elève Commissaire de Police, Ancien Chef de la Brigade de lutte contre la cybercriminalité

– M. Jean-François BEUZE, Président Directeur Général de Sifaris

– M. Ali EL AZZOUI, Président Directeur Général Data Protect

– M. Richard NOUNI, Directeur Général de CFAO Technologies

– Retour d'expériences du secteur bancaire

Questions / Réponses

16h00-16h30

Pause café et visite des stands

16h30-17h30 Plénière 5

Point d'Echange Internet et ouverture du marché des FAI : Vers une amélioration de la qualité de l'Internet au Sénégal ?

Moderateur : M. Mohamadou SAIBOU, Directeur de l'ESMT Dakar

– M. Cheikh BAKHOM, Président de SENIX (Point d'Echange Sénégal)

– M. Tidiane DEBE, Google Afrique

– M. Ali Drissa BADIOEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest

– M. Alex CORENTHIN, Président d'ISOC Sénégal

– Représentant de l'ARTP

Questions / Réponses

17h30-17h45

SDE/Sodeci (Société d'électricité et d'eau de Côte d'Ivoire) face aux enjeux de l'électronique

SEM Sylvestre, Directeur Général de GSZE (Groupement d'intérêt économique de CIE et SODECI).

Clôture

17h45-18h00

DISCOURS DE CLÔTURE

Perspectives sur les enjeux du haut débit mobile au Sénégal avec l'arrivée de la 4G

Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications

PRE-PROGRAMME DU VENDREDI 19 FEVRIER 2015

Réflexion sur Les chantiers de Modernisation de l'administration publique – Trois cas

9h00-9h15 Ouverture

DISCOURS D'OUVERTURE

Par M. Alloune SARR, Ministre du Commerce, du Secteur informel, de la Consommation, de la Promotion des produits locaux et des PME du Sénégal

9h15-10h00 Plénière 1

CAS 1 – SIGIF (Système Intégré de Gestion des Informations financières)

Le SIGIF, un enjeu de modernisation et de transparence dans la gestion des comptes publics

– Gestion intégrée des finances publiques : Retour d'expériences de la Côte d'Ivoire

Par Nongolougo SORO, Directeur Général de la SNDI

– Direction Générale de la comptabilité publique et du Trésor

– M. Ibrahima FAYE, Chef de l'Equipe Projet SIGIF au Ministère de l'Economie des Finances et du Plan

– M. Frédéric MASSE, VP SAP

– M. Jean-Michel MUET, Associé BearingPoint

Questions / Réponses

10h00-11h00 Plénière 2

CAS 2 – GUICHET UNIQUE

Guichet unique et impact sur le Doing business

– Directeur du commerce au Ministère du commerce

– Ibrahima DIAGNE, DG de Gained 2000

– Représentant de l'Apix

– Dr. Alloune DIONE, DSI de la Douane Sénégalaise

Questions / Réponses

11h00-11h20

Pause café et visite des stands

11h20-12h00 Plénière 3

CAS 3 – FICHER D'ETAT CIVIL

Modernisation du Fichier d'état civil, quel enjeu pour la gouvernance locale ?

Moderateur: André GRISSONNANCHE, PDG Evense

– M. Frédéric Massé, VP SAP,

– Mme Emilie Scallier, GDEXpert

– M. Mouhamad Tidiane Seck, Directeur Associé Performances Management Consulting

– Jean-Pierre La Hausse de la Louvière, CEO d'ISTEC

– ADIE

– Ministère de l'Intérieur

– Direction de l'état civil

Clôture

12h00-12h20

DISCOURS DE CLÔTURE

Par M. Abdoulaye Diouf SARR, Ministre de la gouvernance locale, du développement et de l'aménagement du territoire du Sénégal

12h20

Cocktail déjeunatoire



Régalez-vous à cet article

Source : *Programme 6eme Edition IT Forum Senegal – Colloque, Rencontre, IT Forum pour les managers IT africains*

La cybercriminalité obstacle au développement de la Côte d'Ivoire



La
cybercriminalité
obstacle au
développement de
la Côte d'Ivoire

La cybercriminalité constitue un obstacle au développement économique et social des pays africains, d'autant que cela détériore l'image des Etats et freine l'activité des investisseurs. C'est le constat fait par la centaine d'experts réunis depuis lundi à Grand-Bassam, Côte d'Ivoire, dans le cadre d'une Conférence internationale visant le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone.

Organisée par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI), la cérémonie d'ouverture de cette conférence, en présence du ministre d'Etat, ministre de l'Intérieur et de la Sécurité, Hamed Bakayoko, a permis au ministre de l'Economie numérique et de la Poste Bruno Koné de tirer sur la sonnette d'alarme.

Il a en effet appelé les spécialistes des questions de cybersécurité à rester sur le qui-vive, nonobstant le « solde positif » entre les avantages du numérique et les menaces qui en découlent. Difficile de lui donner tort. Le marché ouest-africain de la cybercriminalité parle de lui-même.

En 2013, la Côte d'Ivoire avait été durement touchée par ce fléau, avec une perte de 26 milliards de FCFA. Au Sénégal, on parle d'une perte de 15 milliards de FCFA due à la fraude sur la toile. Suffisant pour installer un climat de méfiance dans les transactions financières électroniques et un défaut de crédibilité face aux investisseurs.

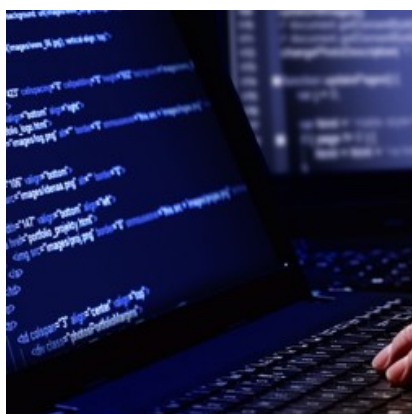
Autant le dire : un plan d'action sur la cybersécurité et la cyberdéfense dans l'espace francophone s'avère nécessaire. Venus d'une vingtaine de pays, les experts présents à cette conférence internationale ont trois jours, pour proposer une stratégie concrète ... [Lire la suite]



Réagissez à cet article

Source : Côte d'Ivoire : plus de 100 experts dénoncent la cybercriminalité comme obstacle au développement | CIO-MAG

La cybersécurité un problème sous estimée par les chefs d'entreprises



La cybersécurité
un problème sous
estimée par les
chefs
d'entreprises

Les entreprises se jugent souvent prêtes à résister aux cyber-attaques alors que la réalité est bien souvent moins reluisante.

Plusieurs études sorties récemment convergent pour montrer un tableau assez catastrophique de la cybersécurité des entreprises alors que la perception affichée par celles-ci est plutôt marquée par l'optimisme. Ou bien faut-il mieux parler d'inconscience ? Ainsi, 62% des entreprises ont déjà subi une tentative de fraude selon une étude de Sage. 12% en ont même subi au moins cinq. La fraude la plus courante reste la fameuse *fraude au président* (usurpation d'identité d'un dirigeant pour obtenir un virement à l'étranger) : 80% des entreprises affectées l'ont rencontrée. 18% ont été victimes d'un *test bancaire* et 14% d'une fraude interne (cas classique : substitution de RIB).

✖ Les trois quarts des DAF craignent avant tout les fraudes d'origines externes. La *fraude au président* et la falsification de RIB sont largement cités avant des cyber-attaques sur des données financières (un quart seulement des répondants). Des processus métier ont été mis en place pour parer ces fraudes non-technologiques comme la séparation créateur/valideur d'un paiement, la double signature... Le respect des procédures et la vigilance interne ont suffi à détecter des fraudes dans de nombreux cas. Mais 30% des entreprises continuent de valider leurs virements par un simple fax ! Suivant les recommandations des organismes professionnels, la bascule vers les traitements informatisés (EBICS TS, via les portails bancaires, etc.) est malgré tout bien engagée.

Une méconnaissance des bonnes pratiques et des règles

Mais il n'en demeure pas moins que la méconnaissance des bonnes pratiques pour sécuriser l'information reste importante. Selon une étude Solucom/Conscio, 46% des collaborateurs ne sont pas préparés à réagir à de l'ingénierie sociale dont la *fraude au président* n'est qu'un exemple caricatural. Pourtant, selon les auteurs de l'étude, l'ingénierie sociale est la méthode principale pour s'introduire dans les systèmes d'information des entreprises ou réaliser des fraudes, notamment par usurpation d'identité ou de couple identifiant/mot de passe.

Si 88% des collaborateurs sont sensibilisés aux règles pour gérer les mots de passe, 47% seulement les adoptent. Un mécanisme technique est donc nécessaire pour obliger à respecter les bonnes pratiques. Enfin, la même étude mentionne que la réglementation sur les données personnelles est méconnue par la majorité des collaborateurs, entraînant de ce fait un important risque juridique pour leurs entreprises.

Bienvenue aux malwares

L'ingénierie sociale est décidément bien ancrée dans les pratiques des cyber-criminels. Cibler précisément les attaques permet notamment, selon l'étude publiée par Cisco, d'introduire des #ransomware. Ce type d'attaque générerait 34 millions de dollars par an et par campagne. Etre victime de tels pratiques est assez gênant, ce qui explique sans doute que seules 21% des entreprises informent leurs partenaires, 18% les autorités et 15% leur compagnie d'assurance. Bien entendu, les fondamentaux du cybercrime sont toujours d'actualité avec des variantes pour les maintenir au goût du jour. La compromission de serveurs est ainsi un classique pour mener des attaques indirectes, notamment via des CMS mal mis à jour. La compromission de domaines WordPress a ainsi augmenté de 221% entre février et octobre 2015. Parmi les mauvaises pratiques qui se développent, la non-mise à jour des infrastructures est en croissance.

La fuite de données via les navigateurs, souvent négligée, est pourtant en pleine croissance : des extensions malveillantes affecteraient 85% des entreprises. Les attaques à base de DNS sont également en plein boom, d'autant que les experts DNS ne travaillent que rarement avec les experts en sécurité. Malgré tout, il est estimé que la rapidité de détection d'une intrusion a augmenté même si elle reste dans une fourchette de 100 à 200 jours.

La cybersécurité sera le sujet de la Matinée Stratégique de CIO le 16 février 2016 : Cybersécurité : Les nouvelles menaces contre le système d'information. ... [Lire la suite]

✖

Réagissez à cet article

Source : *La cybersécurité reste une problématique sous estimée dans les entreprises – Le Monde Informatique*

Quand la machine pourra t-elle dépasser l'homme ?



Quand la machine pourra t-elle dépasser l'homme ?

Face aux progrès déroutants de l'intelligence artificielle, de nombreuses voix s'élèvent et alertent face à l'avènement d'une ère d'asservissement de l'Homme à la machine. En réalité, même si elle a réalisé d'impressionnants progrès, la technologie est encore loin de rivaliser avec l'Homme.

Il existe dans la communauté de l'intelligence artificielle une date qui symboliserait le passage d'une ère d'algorithmes soumis à l'Homme à une ère de machines dominatrices : la « singularité ». Cet instant théorique cristallise les inquiétudes, car les machines, une fois conscientes de leur environnement, seraient capables de se retourner vers leurs créateurs.

Cette panique est encouragée par des discours d'« évangélistes » de l'intelligence artificielle, comme ceux de la Singularity University créée avec le soutien de Google et de la Nasa. Ceux-ci s'attellent à dépasser le monde biologique en repoussant, par exemple, les limites de la mort. Ce transhumanisme prophétique illustre un regain de popularité du progrès technologique après le grand désamour qui avait succédé aux excès guerriers de son usage au début du siècle.

Une avancée sans précédent

L'intelligence artificielle est un des bras armés de la révolution technologique, et ses prouesses ne cessent de surprendre. Le récent « grand bond en avant » vient du passage de programmes aux instructions édités par l'homme, à des programmes « apprenants » où la machine déduit à partir d'exemples les causes d'une conséquence.

Les utilisations commerciales de l'intelligence artificielle sont elles aussi de plus en plus perfectionnées et concernent tous les aspects de la vie d'entreprise. Des start-up proposent à présent des assistants personnels avec qui il est possible de communiquer pour consulter ou modifier un agenda. La voiture automatique de Google se déplace depuis plusieurs années sur les routes américaines et montre un taux d'accidents plus faible d'un conducteur humain .

D'autres algorithmes sont capables de proposer les meilleurs itinéraires en temps réel en prenant en compte la circulation actuelle, et enfin, l'intelligence artificielle s'est récemment illustrée en battant les plus grands joueurs de Go , considéré comme l'un des jeux les plus difficiles.

La limite de l'excellence

Ces impressionnantes performances cachent en réalité la plus grande limite de l'intelligence artificielle, son excellence à réaliser une tâche particulière, et non un ensemble de tâches. L'Homme, s'il ne peut exceller dans tous les domaines, doit cette imperfection à sa capacité d'adaptation.

Notre propension à faire des erreurs témoigne de notre capacité à nous adapter au monde qui nous entoure et à rechercher des solutions innovantes à chaque problème. Cette capacité d'adaptation à l'environnement manque aujourd'hui à l'intelligence artificielle.

Une autre des grandes limites du Machine Learning tient de sa nécessaire interaction avec l'Homme. Si la machine est aujourd'hui capable d'étudier les relations entre plusieurs variables, de choisir les paramètres les plus judicieux à la résolution d'un problème, elle n'est en revanche pas capable d'imaginer à priori quels éléments utiliser et de les rechercher de façon proactive.

Par exemple, la reconnaissance d'objets sur photos demande d'effectuer de nombreux tests et de comparer plusieurs modèles. Le rôle de l'Homme est ici de rechercher les variables explicatives (couleurs des pixels, interactions entre certains éléments de l'image, etc.) et de demander à l'algorithme d'évaluer leur importance statistique.

Une logique trop fidèle au cerveau humain

Un des freins au progrès sans fin de l'intelligence artificielle tient de sa méthode de conception. C'est souvent du fonctionnement du cerveau humain que les chercheurs s'inspirent pour résoudre les problèmes les plus complexes.

Or, il est difficile d'imaginer des méthodes de réflexions dépassant l'expérience que nous avons du raisonnement logique. De plus, le cerveau humain est à notre connaissance l'ordinateur le plus performant, et la technologie actuelle est à des lieux de pouvoir le recréer.

Sa capacité de stockage, souvent révisée, est aujourd'hui estimée à 1 petabyte, soit 1.000.000 de gigabytes, où la capacité d'environ 2.000 ordinateurs actuels. Sa vitesse de traitement d'opérations et elle aussi remarquable, et sa capacité d'adaptation est telle qu'il est impossible de l'imaginer d'un point de vue algorithmique.

Un danger organisationnel

Le futur de l'intelligence artificielle ne sera donc pas dans un asservissement de l'Homme par la machine, mais dans une plus grande association entre le créateur et son outil. Elle doit, en revanche, nous faire réfléchir à notre place dans la société et dans l'entreprise. Si les hommes ne sont aujourd'hui pas physiquement menacés par l'intelligence artificielle, son avènement entraînera une transformation radicale de l'organisation et de la répartition du travail.

De nombreux emplois et services seront remplacés par des algorithmes intelligents et autonomes. Ainsi, le plus grand défi de la société face à l'intelligence artificielle sera de repenser le rôle de chacun, et d'adapter tous les acteurs de l'économie à cette transformation.

Par **Jonathan Trevier**, fondateur de Sparkism



Réagissez à cet article

Source : *L'Homme dépassé par la machine, ce n'est pas pour demain, Le Cercle*