

# TechnoMagazine

Le Magazine NTIC au Maroc [www.TechnoMag.ma](http://www.TechnoMag.ma)

Non destinée  
à la vente  
**GRATUIT**

## Insécurité du système d'information



Numéro 17 - Juin 2012 - TechnoMag votre magazine gratuit des nouvelles technologies



**Logiciel : p. 16**

**Data Loss/Leak  
Prevention (DLP)**

**Interview : p. 20**

**M. Julien PULVIRENTI  
de Kaspersky**



**Entreprise : p. 28**

**Comment se préparer  
à la loi 09-08**

# 250



nouveaux appareils mobiles  
à prendre en charge

# 30



employés désirant accéder  
aux données de l'entreprise avec  
leur tablettes flambant neuves

# 20



applications accessibles  
depuis le nuage

# 100



nouveaux miracles  
à accomplir aujourd'hui

## Be Ready for What's Next.

### Voici Kaspersky Endpoint Security suite.

Que ce soit pour prêter assistance à vos employés mobiles avec leurs tablettes personnelles ou pour placer des applications et des données essentielles dans le nuage, vos activités évoluent rapidement. Ces changements apportent leur lot de nouveaux risques informatiques sans précédents pour la sécurité.

Contrairement aux autres protections de terminaux disponibles aujourd'hui, Kaspersky Endpoint Security 8 et Kaspersky Security Center 9 ont été élaborés sur mesure. Une solution transparente. Une solution dotée de nombreuses innovations, assurant une protection intelligente et un contrôle remarquable de votre environnement informatique afin de réduire les risques dans votre monde en évolution permanente.

**Et n'oublions pas le meilleur : cette solution vous est proposée par le leader mondial en matière de lutte contre les logiciels malveillants, Kaspersky Lab.**

[kaspersky.fr/beready](http://kaspersky.fr/beready)

**KASPERSKY** lab

**DIRECTION  
DIRECTEUR DE LA PUBLICATION**

Mounaim Elouazzani  
elouazzani@technomag.ma

**RÉDACTION**

Mounaim Elouazzani  
elouazzani@technomag.ma

**DIRECTION COMMERCIALE**

Samira Amsoul  
samira@technomag.ma  
Gsm: 06 66 89 44 99

**P.A.O**

Saad Rachid  
saad@technomag.ma

**IMPRESSION**

Edit, Casablanca

**Technomag est édité par:**

Technomagazine S.A.R.L.  
47, Bd Mohamed Ben Abdellah,  
Résidence Belle Vue, 2ème étage, Bureau 182.  
Casablanca, Maroc.  
Tél. : 0522 47 39 31  
Fax : 0522 44 99 26  
E-mail : contact@technomag.ma  
siteweb : www.technomag.ma

Dépôt légal : 2011TE0019  
ISSN : 2028-473X



<http://www.facebook.com/TechnoMagazine>  
[http://twitter.com/#!/TechnoMag\\_maroc](http://twitter.com/#!/TechnoMag_maroc)

Vos conseils et remarques sont les bienvenus !



**Mounaim ELOUZZANI**  
elouazzani@technomag.ma

*L'informatique connaît des évolutions permanentes depuis des années mais rarement des changements majeurs.*

*Les problèmes de sécurité autrefois réservés aux PC s'attaquent maintenant à tout le High-tech: Les tablettes et les Smartphones ne sont plus épargnés par les virus. Même les Mac, annoncés comme sécurisés ne sont plus à l'abri, un virus majeur ayant touché récemment plus de 500 000 Mac dans le monde.*

*Ce phénomène de cybercriminalité qui monte en puissance est expliqué par le nombre exponentiel des internautes qui a doublé depuis 2008. En outre, l'ADSL, la démocratisation des terminaux et la diffusion des hackers toolkits ont suscité des vocations en leur donnant des outils suffisamment puissants pour réaliser des actions illicites. Même des acteurs de la lutte anti-piratage comme Panda Security ou RSA ont été frappés. Et, avec 17 milliards de matériels connectés, les occasions ne manquent pas pour voler le contenu qu'ils recèlent.*

*En plus, il y a les effets de la crise financière que se font sentir et qui poussent les entreprises à réduire leurs budgets informatiques ainsi que leurs dépenses en infrastructures de sécurité. Mais, aussi tentant que cela puisse être, économiser sur les budgets de sécurité de l'information s'avère déraisonnable. Si l'entreprise baisse sa garde, des individus malintentionnés en profiteront pour exploiter les failles résultant de ces mesures «d'économie».*

*Face à ces menaces, les entreprises et leurs DSI disposent heureusement d'une multitude de parades logicielles et matérielles qui, avec une politique sécuritaire pragmatique, sont à même d'assurer une protection efficace de l'infrastructure IT*

**“ Ce phénomène de cybercriminalité qui monte en puissance est expliqué par le nombre exponentiel des internautes qui a doublé depuis 2008 ”**



**Spécial Serveurs et Desktops**  
(Interviews, analyses, chiffres clés, etc.)

✓ Bouclage le lundi 25 juin 2012

## ACTUALITÉS

- 5- McAfee dévoile la nouvelle génération des solutions SIEM
- 6- Un Mac sur 5 infecté
- 6- NetApp : très bons résultats au quatrième trimestre de son année fiscale
- 7- Kaspersky Lab lance une nouvelle solution de sécurité pour les tablettes Android
- 8- Inwi « Solutions Entreprises » innove avec ses nouveaux Forfaits mobiles
- 10- Le marché de L'UTM dépasse le milliard de dollars
- 10- Touch Media partenaire de Google au Maghreb
- 11- Bitdefender optimise les performances de votre appareil Android gratuitement
- 12- Sophos assure la sécurité sur Facebook
- 12- Sécurité maximale de Juniper Networks pour les terminaux mobiles
- 12- McAfee et Intel s'unissent pour la protection du secteur de l'énergie

## TÉLÉCOM

- 13- Résultats de l'enquête de collecte des indicateurs TIC 2011

## INFRASTRUCTURE

- 14- UTM les appliances de sécurité multifonctions

## LOGICIELS

- 16- DLP: Data Loss/Leak Prevention
- 17- Seconde année de hausse pour les logiciels de gestion des IT

## ÉVÈNEMENT

- 18- Nexans sponsor du Alcatel-Lucent Enterprise Dynamic Tour

## INTERVIEW

- 20- M. Julien PULVIRENTI Territory Sales Manager de Kaspersky

## SÉCURITÉ

- 22- Le lancement de l'IPv6 révèle des défis de sécurité
- 23- Quelles solutions pour lutter contre la fraude en ligne ?
- 24- Les Advanced Evasion Techniques ou AET
- 26- Flame serait-il le maliciel le plus complexe ?

## ENTREPRISE

- 27- Gestion Globale des Risques
- 28- Données à caractère personnel : la loi 09-08 ?

## INNOVATION

- 30- La logique Cloud et SaaS pour la PME marocaine
- 31- Entretien avec Driss LEBBAT D.G, ADK Media

## ASTUCES

- 32- Comment protéger les utilisateurs des réseaux sociaux
- 32- Lancer un sondage sur Facebook

## WEB

- 34- Un site populaire ne veut pas dire un site sécurisé

# McAfee dévoile la nouvelle génération des solutions de gestion des événements et des risques de sécurité SIEM

**McAfee**  
Proven Security™

La prochaine génération SIEM (Security Information and Event Management), intégrée aux solutions McAfee ePolicy Orchestrator, McAfee Risk Advisor et McAfee Global Threat Intelligence, fournira aux utilisateurs une visibilité et une gestion sans précédent.

Cette solution de cartographie des risques de sécurité SIEM au travers de McAfee Enterprise Security

Manager (autrefois NitroView) fait évoluer le SIEM d'un simple analyseur d'événements en un outil granulaire et intelligent de détection dynamique des risques en entreprise.

McAfee Enterprise Security Manager cartographie les risques de sécurité grâce à l'analyse des logs concernant les événements, utilisateurs, systèmes, données et risques et les corrèlent en vue de fournir des informations pointues. Cela permet de dresser un inventaire précis, et en temps réel, des menaces à partir de McAfee Global Threat Intelligence et de déterminer ainsi la conformité des procédures de sécurité et les contre-mesures au travers de la plate-

forme McAfee ePolicy Orchestrator et de McAfee Risk Advisor. Cette compréhension intelligente de la sécurité, en reliant les points et en identifiant les attaques, permet de réduire le temps de réponse et de fournir des alertes de sécurité prioritaires intelligentes. ■



## SOLUTIONS ENTREPRISES

### TÉMOIGNAGE

« Notre chargée de compte chez inwi se préoccupe avant tout de nos problèmes avant de promouvoir ses produits »

Salim EL JAI

Directeur de développement des ventes

**MICRODATA**  
CONSEIL - INFRASTRUCTURES - INTÉGRATION DE SERVICES

Microdata est une entreprise qui compte 130 employés travaillant essentiellement dans l'intégration d'infrastructure IT. La société est installée sur 9 sites à travers le Maroc.

Quelles sont les solutions mobile inwi pour lesquelles vous avez opté ?

Nous avons opté pour une flotte de téléphones portables de près de 120 lignes pour nos équipes commerciales ainsi que pour notre staff technique.

Pourquoi une bonne qualité de couverture réseau est-elle importante dans votre secteur d'activité ?

La téléphonie, de manière générale, reflète un peu l'image de notre entreprise. Par conséquent, il est très important que la qualité du réseau ne vienne pas dégrader notre image.

Depuis que nous sommes engagés avec inwi, la qualité du réseau mobile s'est considérablement améliorée.

Comment jugez-vous le service clientèle chez inwi ?

Pour moi, la particularité du service clientèle inwi, c'est l'interlocuteur unique. Nous avons une chargée de compte qui s'occupe de nos requêtes. Elle se préoccupe avant tout de nos problèmes avant de promouvoir ses produits.

Je me sens privilégié, rassuré, parce que je n'ai pas l'impression de devoir tout réexpliquer à chaque fois que je suis en contact avec le service clients de inwi.

Retrouvez l'intégralité de l'interview sur : [www.inwi.ma/entreprises](http://www.inwi.ma/entreprises)

Profitez à votre tour des Solutions Entreprises de inwi appelez le 05 29 10 10 10

**inwi**  
عبر كبعيتي

## Un Mac sur 5 infecté

**L**es Mac sont-ils vraiment épargnés par les virus et les malwares ? Apparemment, non selon Sophos qui révèle dans une étude qu'un Mac sur cinq serait infecté par un malware.

Après avoir analysé 100 000 ordinateurs Mac équipés de son logiciel antivirus gratuit, Sophos s'est aperçu que 20% des Mac possédaient une ou plusieurs "instances" de malwares ciblant Windows. Alors évidemment, sur Mac, ces malwares PC ne sont absolument pas dangereux (excepté si le Mac possède une partition PC), mais le risque de diffusion à d'autres ordinateurs persiste.

Cette analyse a par ailleurs montré que 2,7% des Mac étaient porteurs d'un logiciel malveillant Mac OS X. Certains utilisateurs de Mac se sentent rassurés sachant qu'il existe sept fois plus de probabilités que leur ordinateur soit infecté par des virus, des logiciels espions et des chevaux de Troie Windows que par un logiciel spécifique Mac OS X. Or, il devient malheureusement de plus en plus fréquent de rencontrer des logiciels malveillants de type Mac. Les utilisateurs doivent être conscients de l'émergence de cette menace.

Sophos précise que le paysage des menaces ciblant les Mac est dominé par les attaques à l'aide de faux antivirus, amenant l'utilisateur à communiquer ses données bancaires. Le plus embêtant pour Sophos c'est que même certains Mac (1 sur 36) équipés de son logiciel Sophos Anti-Virus Home Edition ont quand même été infectés par un malware de type Mac. Le hit parade des malwares Mac étant, dans l'ordre : OSX/Flshplyr (75,1%), OSX/FakeAV (17,8%), OSX/RSP1ug (5,5%), OSX/Jahlav (1,2%).

Graham Cluley rappelle que "les logiciels malveillants qui ciblent les Mac peuvent être diffusés par le biais d'une clé USB, d'une pièce jointe à un e-mail, d'un téléchargement sur un site Web ou d'une installation insidieuse, sans même que l'utilisateur s'aperçoive que la sécurité de son Mac a été compromise". Pour les cybercriminels, les Mac sont des cibles rares mais privilégiées, car les propriétaires utilisent rarement un logiciel antivirus et sont supposés avoir des revenus supérieurs à ceux de l'utilisateur Windows type. Voilà pourquoi Sophos conseille à tous les utilisateurs de Mac se protéger sans attendre. ■

## NetApp enregistre de très bons résultats au quatrième trimestre de son année fiscale



**R**ésultats du quatrième trimestre encourageants, chiffre d'affaires annuel exceptionnel : le vendeur de solutions de stockage NetApp termine l'année fiscale 2011 à la hausse. Avec un chiffre en illustration : son chiffre d'affaires annuel a augmenté de plus d'un milliard de dollars par rapport à 2010.

NetApp vient de publier au titre de son quatrième trimestre fiscal, un bénéfice de 181 M\$ et 47 cents par titre contre 161 M\$ et 40 cents par action un an avant. Les revenus totalisent 1,7 Md\$ contre 1,43 Md\$ un an plus tôt. Le bpa ajusté ressort à 66 cents. Le consensus tablait sur un bpa de 63 cents pour des ventes de 1,68 Md\$ ce qui représente une hausse de 30% de son chiffre d'affaires, et de 38% de son avoir bancaire au cours de l'année fiscale 2011.

"Les clients peuvent profiter énormément de la virtualisation de stockage dans leurs DCs afin de gagner en efficacité, flexibilité,

et économie des coûts... NetApp fournit la proposition la plus convaincante dans l'industrie pour les déploiements de Cloud privés et publics" a déclaré Tom Georgens, président et chef de la direction. « Notre succès est évident dans nos résultats, comme NetApp a remporté un nombre record de nouveaux clients, une augmentation significative de nos unités expédiées, y compris un nombre record de systèmes haut de gamme, et a connu une croissance solide des revenus dans presque toutes les zones géographiques en troisième trimestre »

Ces bons résultats permettent au fabricant d'envisager le début d'année 2012 sous les meilleures auspices : il s'attend à un chiffre d'affaires de 1,5 milliard de dollars pour le premier trimestre 2012, à plus ou moins 3%, ce qui correspondrait à une hausse de près de 26% par rapport au premier trimestre 2011. ■

## Kaspersky Lab lance une nouvelle solution de sécurité pour les tablettes Android

L'éditeur de solutions de sécurité informatique annonce le lancement de Kaspersky Tablet Security.

Tout en assurant la protection contre les virus et autres malwares, le logiciel tient également l'utilisateur à l'écart des sites Web dangereux, en particulier ceux qui cherchent à s'approprier les identifiants des comptes de réseaux sociaux ou de banque en ligne.

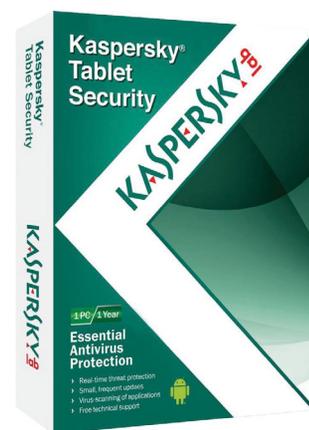
Cerise sur le gâteau : grâce à une technologie innovante, les victimes d'un vol de leur tablette peuvent activer via le web la nouvelle fonction Mugshot, qui permet de prendre secrètement une photo de la personne utilisant leur appareil. Le logiciel envoie ensuite ce cliché au propriétaire légitime, qui peut alors le communiquer aux autorités compétentes. Le programme peut également bloquer ou effacer à distance

une tablette perdue ou volée, de façon à sécuriser l'ensemble des e-mails, documents et clichés personnels qu'elle contient.

Selon Victor Dronov, responsable produit de Kaspersky Lab, « Le nombre d'appareils que nous utilisons dans notre vie quotidienne va sans cesse croissant et la possibilité d'accéder à Internet via différentes plates-formes constitue indubitablement une fantastique ressource. Cependant, en cas de perte d'un mobile, toutes nos données personnelles peuvent se trouver menacées : e-mails, identifiants d'accès aux réseaux sociaux, mots de passe, coordonnées bancaires, etc. Par ailleurs, des programmes malveillants et frauduleux peuvent également causer des dommages considérables voire un préjudice financier. Avec Kaspersky Tablet Security, les utilisateurs peuvent oublier ces risques et

goûter pleinement aux joies de la mobilité numérique. »

Kaspersky Tablet Security est disponible à la fois sur le site mondial de Kaspersky Lab et sur Android Market, pour les tablettes dotées d'Android OS 2.x-4.x. ■



### SOLUTIONS ENTREPRISES

#### TÉMOIGNAGE

« Nous arrivons à joindre facilement tous nos collaborateurs quel que soit le site dans lequel ils se trouvent »

Khalid AGGADI  
Directeur financier et de l'organisation



Atlas Voyage est une entreprise du secteur du tourisme. Elle compte 300 collaborateurs implantés essentiellement à Casablanca et à Marrakech, ainsi qu'un réseau d'une douzaine d'agences à travers tout le Maroc.

#### Quelles sont les solutions inwi pour lesquelles vous avez opté ?

Nous avons opté pour une solution mobile forfaitaire de près de 400 lignes mobiles sachant que notre compagnie, du fait de son activité, travaille avec un certain nombre d'agents qui sont amenés à se déplacer très souvent.

Cette solution nous permet de nous assurer de la disponibilité des salariés qui doivent être joignables à tout moment mais aussi de faire des gains considérables en matière de coût et de facturation.

#### Pourquoi une bonne qualité de couverture réseau est-elle importante dans votre secteur d'activité ?

La qualité réseau est très importante car dans notre secteur, nous avons l'obligation de rester en contact avec nos collaborateurs qui encadrent des groupes à travers tout le pays.

Nous devons toujours répondre aux exigences particulières de nos clients, où qu'ils soient et à n'importe quel moment du jour ou de la nuit, la communication ne doit jamais être coupée.

#### Êtes-vous satisfait du réseau inwi ?

Oui, nous sommes pleinement satisfaits du réseau inwi.

Nous avons une bonne couverture réseau, nous arrivons à joindre facilement tous nos collaborateurs quel que soit le site dans lequel ils se trouvent.

Retrouvez l'intégralité de l'interview sur : [www.inwi.ma/entreprises](http://www.inwi.ma/entreprises)

Profitez à votre tour des Solutions Entreprises de inwi  
appelez le 05 29 10 10 10

inwi  
عبر كبعيتي

# Inwi « Solutions Entreprises » innove avec ses nouveaux Forfaits mobiles



**F**idèle à son engagement de faire de l'activité « Entreprise » un axe de développement stratégique pour l'année 2012, inwi lance de nouveaux Forfaits au sein de sa gamme « Solutions mobiles Entreprises ».

L'opérateur a ainsi revu la tarification de ces forfaits avec, à la clé, un vrai choix offert aux entreprises pour répondre à leurs besoins comme, par exemple, pouvoir bénéficier de vrais bonus 24h/24 et 7j/7, même à l'international et sans avoir à subir le désagrément d'heures superflues.

Les Forfaits Open de notre gamme mobile font peau neuve pour le plus grand bénéfice des entreprises. inwi, opérateur global et alternatif de télécommunications, vient en effet de lancer une nouvelle formule de ces Forfaits, avec une tarification avantageuse revue à la baisse permettant aux dirigeants d'entreprises et à leurs équipes de s'exprimer comme ils le souhaitent. Une offre qui est le fruit de l'écoute permanente du marché des Entreprises afin de lui apporter les solutions qui répondent à ses vrais besoins de communication.

« Cette initiative traduit notre ferme volonté, solennellement exprimée en mars dernier, d'être un acteur majeur du marché des Entreprises, combien stratégique pour le développement du secteur des télécommunications au Maroc », explique à cet effet Frédéric Debord, Directeur Général de inwi. Pour rappel, l'opérateur avait en effet affiché son engagement à faire de l'activité « Entreprise » un axe de développement prioritaire pour cette année 2012, à travers la création d'une nouvelle entité dédiée à ce segment et la nomination à sa tête d'un professionnel connu et reconnu des TIC, Mehdi Kettani.

Plusieurs semaines durant, nos équipes sont allées à la rencontre de chefs d'entreprises qui, à notre grande satisfaction, reconnaissent unanimement aujourd'hui à inwi son statut d'opérateur global des

télécommunications au Maroc et lui renouvellent leur expression de confiance. Les différents témoignages recueillis à cette occasion -et qui donneront d'ailleurs le coup d'envoi de notre campagne de communication autour de la nouvelle offre- traduisent en effet la satisfaction des chefs d'entreprises quant à la qualité de notre service client et nos procédures souples de portabilité. L'opérateur s'appuie par ailleurs sur une grande crédibilité acquise auprès des entreprises comme partenaire de référence dans le domaine de transfert de données à très haut débit et de l'internet (Data).

## Les nouveaux Forfaits Open : le vrai prix pour les vrais besoins

Suite à l'écoute attentive du marché, inwi a donc substantiellement revu la tarification de ses Forfaits Open GSM dédiés aux entreprises, dans l'objectif de proposer le juste prix correspondant à des besoins réels de communication. Inwi donne également satisfaction aux dirigeants qui souhaitent ne plus être encombrés par des heures de communication ou encore des bonus inutiles. Notre nouvelle gamme des forfaits Open offre à cet effet de vrais bonus 24h/24 et 7j/7, même à l'international et sans heures superflues. Des forfaits disponibles à partir de 100 dhs, garantissant l'intra-flotte gratuite, illimitée et sans conditions et proposant le paiement à la seconde en option.

Ainsi, afin de permettre aux entreprises de réellement choisir de payer moins pour consommer ce qu'elles choisissent de consommer, **inwi enrichit la gamme Open par la création de deux nouveaux forfaits :**

- **Un forfait offrant 1 heure de communication en crédit principal et 1 heure de bonus, à 100 dhs HT.**
- **Un forfait offrant 3 heures de communication en crédit principal ainsi qu'1 heure de bonus ; à 120 dh HT.**

A noter aussi que inwi apporte davantage de générosité pour les autres forfaits Open déjà existants sur le marché. En effet, les forfaits de 2h30 à 6h30 (inclus) se voient enrichis d'1 heure et 30 minutes de communications gratuites, ainsi qu'1 heure de bonus gratuit. Les forfaits de 11h à 20h

se voient ajouter quant à eux 2 heures de communications et donnent l'équivalent du forfait en bonus.

Cerise sur le gâteau, l'ensemble des bonus offerts donne désormais droit aux communications internationales de la zone (Belgique, Espagne, France, Italie & Pays-Bas).

Avec le lancement de sa nouvelle gamme des Forfaits Open, inwi réaffirme sa volonté de contribuer activement à l'essor de notre tissu économique, dont le développement demeure intimement lié aux télécommunications à l'heure de la mondialisation. Une nouvelle initiative de inwi pour permettre aux chefs d'entreprises et à leurs collaborateurs de s'exprimer comme ils le souhaitent, toujours au nom d'une approche simple et audacieuse.

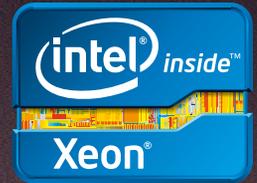
## Les « Solutions mobiles entreprises » : quand l'offre s'adapte aux attentes

Dans une entreprise, chaque collaborateur a sa façon de téléphoner. Avec ses solutions mobiles dédiées, inwi propose à chaque entreprise de composer une flotte sur mesure et de choisir pour chacun de ses collaborateurs le forfait qui est le mieux adapté à ses besoins de communication :

- **Forfaits Communauté: appels illimités(\*) vers tous les mobiles inwi**
- **Forfaits Open: gratuits 24h/24 et 7j/7 vers tous les opérateurs**
- **Plan Executive: l'utilisateur ne paye que ce qu'il consomme**

Ces forfaits offrent une palette d'avantages: appels vers les fixes et mobiles internationaux en Europe de l'Ouest, Maghreb et Amérique du Nord au tarif national ; l'intra-flotte gratuit et illimité, sans condition ; la tarification à la seconde en option pour les forfaits ainsi que l'internet sur mobile gratuit et illimité. En plus, la portabilité est garantie en toute souplesse, puisque les collaborateurs des entreprises peuvent changer vers inwi, tout en conservant leurs numéros de téléphone.

(\*) 60h pour les forfaits 2h30, 4h30 et 100h pour les forfaits de 6h30 et plus. ■



# Une grande puissance implique de grandes opportunités..



## Métamorphosez votre entreprise avec les nouvelles solutions de datacenter de 12e génération.

Ne laissez pas de place au hasard dans la réussite de votre entreprise. Dotez votre service informatique d'un avantage concurrentiel avec les toutes nouvelles solutions de serveurs Dell™ PowerEdge™, optimisés par les processeurs Intel® Xeon®. Vous détiendrez ainsi l'efficacité, la flexibilité et la fiabilité nécessaires pour surmonter vos plus gros défis. Ces serveurs font partie de la large gamme de solutions de datacenter de bout en bout proposées par Dell pour offrir à votre entreprise tout ce dont elle a besoin, et plus encore.



The power to do more

Visitez [YourDellSolution.com/ma](http://YourDellSolution.com/ma)

©2012 Dell Products. Dell, le logo Dell et PowerEdge sont des marques commerciales déposées ou non déposées de Dell Inc. aux États-Unis et dans d'autres pays. Intel, le Logo Intel, Xeon et Xeon Inside sont des marques de commerce d'Intel Corporation aux États-Unis et dans d'autres pays. D'autres marques de commerce ou noms de marques peuvent être utilisés dans ce document en référence à des produits tiers (systèmes d'exploitation et logiciels) compris dans les produits proposés par Dell et par les entités détentrices des marques et des noms de marques de leurs produits. Dell renonce à tout intérêt de propriété des noms et marques de tiers.

Dell Corporation Ltd, Dell House, The Boulevard, Cain Road, Bracknell, Berkshire, RG12 1LF.

## Le marché de L'UTM dépasse le milliard de dollars

1,16 milliard de dollars. C'est ce qu'a pesé l'an dernier le marché de l'UTM (UnifiedThreat Management). Un marché qui a d'ailleurs affiché une croissance de 19,6%.

"Le marché de l'UTM est en pleine transition" explique Lawrence Pingree, Directeur de recherche chez Gartner, "les clients passant de technologies anciennes, comme les pare-feux dynamiques, à des solutions d'inspection nouvelle génération supportant notamment le contrôle d'applications". Sur ce marché, Fortinet est le numéro 1 du secteur avec un chiffre d'affaires de 228 millions de dollars, en hausse de 33% par rapport à 2010 et une part de marché de 19,6%. SonicWALL, le numéro 2, relativement loin derrière avec 154 millions de dollars de chiffre d'affaires (+16,1%) et 13,3% de parts de marché. Puis 4 fournisseurs se tiennent dans un mouchoir de poche : Juniper Networks (138 millions de dollars de chiffre d'affaires, +7,7%), CheckPoint Software (127 millions de dollars, +15,7%), WatchGuard (127 millions de dollars, +13,5%) et Cisco (107 millions de dollars, +7,1%).

Le marché le plus développé est évidemment le marché nord américain. Il génère 431 millions de dollars de revenus (+15,5% par rapport à 2010) avec en guise de locomotives le secteur bancaire et l'industrie du paiement par carte.

L'Europe de l'Ouest est le second marché avec 310 millions de dollars de chiffre

d'affaires l'an dernier (+16,7% par rapport à 2010). L'Europe de l'est (28 millions de dollars de CA), la zone MEA (28 millions de dollars de CA également), le Japon (32 millions de dollars de CA), la zone Asie/Pacifique (204 millions de dollars de CA) et l'Amérique latine (45 millions de dollars de CA) sont également des marchés en pleine croissance.

Top 10 Worldwide Unified Threat Management (SMB Multifunction Firewalls) Vendors' Revenue for 2011 (Millions of US Dollars)

Company	2011 Revenue	2011 MarketShare (%)	2010 Revenue	2010 MarketShare (%)	2010-2011 Growth (%)
Fortinet	228	19.6	172	17.6	33.0
SonicWALL	154	13.3	133	13.7	16.1
Juniper Networks	138	11.8	128	13.2	7.7
CheckPoint Software Technologies LTD	127	10.9	110	11.3	15.7
WatchGuard Technologies	127	10.9	112	11.5	13.5
Cisco	107	9.2	100	10.3	7.1
Sophos (Astaro)	73	6.3	54	5.6	35.5
SECUI	52	4.4	33	3.3	58.8
Cyberoam	47	4.0	35	3.6	32.5
Barracuda Networks	40	3.4	36	3.7	10.8
Other Vendors	71	6.1	60	6.0	18.3
Total	1,163	100.0	972	100.0	19.6

Source: Gartner (March 2012)

## Touch Media partenaire de Google au Maghreb

- Touch Media, première régie à proposer DoubleClick Ad Exchange (AdX) de Google

Touch Media, acteur de premier plan du secteur de la communication en ligne au Maroc, annonce son partenariat avec Google pour offrir les solutions DoubleClick Ad Exchange (AdX) de Google pour la première fois au Maghreb.

Cette offre vient compléter Touch Premium, le service de vente de solutions publicitaires sur internet en réseaux de sites thématiques de Touch Media, permettant d'augmenter les revenus publicitaires des partenaires éditeurs de Touch Media.

Les réseaux Touch Premium permettent d'employer des formats publicitaires Rich Media, tels que

l'inVideo, consistant à placer des vidéos en ligne sur les bannières, ou l'expand banner, qui consiste en une bannière qui s'agrandit pour révéler plus de contenu au passage de la souris. L'offre comprend également le format propriétaire exclusif développé par Touch Media nommé



le « Buzz Banner™ », permettant d'accroître sensiblement l'influence de l'annonceur sur les réseaux sociaux, et peut être déployée sur des sites marocains à forte fréquentation tels que Viadeo, Soukaffaires, Radiomars, Telquel-online, Moteur.ma et Almountakhab.

« Nos clients ont toujours cherché à trouver des solutions publicitaires digitales efficaces, tout en souhaitant associer leur images de marque à des supports de prestige. », a déclaré Mohamed Mezian, directeur administrateur général de Touch Media. « A présent, ils peuvent faire les deux en même temps avec Touch Premium ».

### A propos de Touch Media

Fondée en 2009, Touch Media s'est rapidement imposée en tant qu'acteur majeur dans le secteur de la communication en ligne au Maroc.

Les métiers de Touch Media couvrent l'ensemble des besoins en communication internet de ses clients: Conseil digital, achat média online, conception, développement et maintenance de contenu. ■

## Bitdefender Power Tune-Up optimise les performances de votre appareil Android... gratuitement



Avec Power Tune-Up, gardez le contrôle de votre tablette et smartphone Android. Suite au succès mondial des tests réalisés en version bêta, Bitdefender annonce la mise à disposition de Power Tune-Up, une application gratuite qui permet d'améliorer les performances de votre Android tout en préservant la batterie et en contrôlant le trafic de données.

Power Tune-Up, la dernière application de l'éditeur antivirus Bitdefender, permet de suivre le trafic de données grâce à des alertes et à des seuils que l'on peut définir soi-même. Il libère de l'espace dans la mémoire interne ainsi que sur les cartes SD internes et externes pour profiter au maximum des performances de son appareil et permet de l'utiliser en toute tranquillité grâce à son option Économiseur de batterie. En bref, il améliore en quelques clics les performances et vous permet de profiter plus longtemps de votre appareil Android.

« Bitdefender renforce ses offres de services pour périphériques mobiles avec cet outil gratuit extrêmement utile pour appareils Android » déclare Fabrice le Page, Chef de Produits Bitdefender chez Editions Profil. « Power Tune-Up fait un excellent travail, en réduisant la consommation du processeur et l'impact sur la batterie. Il fait partie des applications de premier choix de Bitdefender pour appareils mobiles » ■



Load balancing

Haute disponibilité UTM

Encryption

Filtrage

Sauvegarde

Authentification

WIFI

Sécurité

Antivirus

Antispam

Accélération

**Votre Distributeur  
Expert Réseaux  
et Sécurité**

## Sophos assure la sécurité sur Facebook



**S**ophos devient partenaire de Facebook. Sa mission : protéger les utilisateurs contre les liens pointant vers des malwares ou des sites pirates.

Facebook n'est pas un endroit sûr. Ce n'est une surprise pour personne. Alors pour changer un peu la donne, le réseau social utilisera d'ici peu le service de réputation de sites Web des SophosLabs afin d'analyser les liens Web circulant au malveillant. Et ce, en plus de ses propres outils de sécurité. "Notre objectif est toujours de mieux protéger nos utilisateurs, qu'ils soient sur Facebook ou non" a expliqué Joe Sullivan, responsable de la sécurité, Facebook. "En incorporant les informations et l'expertise de pointe de Sophos en matière de sécurité informatique, nous garantirons encore plus de sécurité à nos utilisateurs".

Derrière le discours, les actes. Dès aujourd'hui donc, les SophosLabs enrichiront la base de données de renseignements de Facebook concernant les URL malveillantes. Ainsi, si un lien s'avère vérolé, l'utilisateur qui a cliqué dessus en sera averti par Facebook puis redirigé vers une page lui proposant trois options: continuer à ses propres risques ; retourner à l'écran précédent ; ou bien obtenir de plus amples informations sur la raison pour laquelle le lien a été signalé comme suspect.

Les utilisateurs de Mac auront même la possibilité de télécharger le logiciel gratuit Sophos Anti-Virus pour Mac Édition familiale sur la page Facebook de Sophos. Un joli coup de pub pour Sophos. ■

## Sécurité maximale avec l'offre Simply Connected de Juniper Networks pour les terminaux mobiles

**J**uniper Networks annonce de nouveaux ajouts à son offre Simply Connected qui simplifient et sécurisent l'accès des terminaux mobiles aux réseaux des entreprises. Disponibles immédiatement, ces solutions permettent d'unifier, d'automatiser et de simplifier l'application des règles de sécurité d'entreprise.

Les administrateurs IT peuvent ainsi définir des règles de sécurité et de contrôle des accès cohérentes et étendues tant aux réseaux sans fil que filaires, pour les terminaux personnels des collaborateurs, ceux des visiteurs, et ceux de l'entreprise, et les faire appliquer de manière automatique. Cette nouvelle approche réduit la complexité de la gestion et de l'application des règles de contrôle d'accès pour les administrateurs IT confrontés au phénomène du BYOD (bring-your-own-device). ■

## McAfee et Intel s'unissent pour la protection des infrastructures du secteur de l'énergie

**M**cAfee et Intel ont collaboré conjointement au développement d'un plan visant à protéger les infrastructures énergétiques. A travers ce partenariat, McAfee et Intel s'engagent à mieux protéger des cyber attaques l'écosystème mondial pour l'utilité énergétique, incluant la production, la transmission et la distribution. McAfee et Intel ont présenté un « programme de référence » qui intègre une solution complète de différents produits destinés à créer de multiples couches de sécurité et à fonctionner ensemble sans grande complexité et sans impact sur la disponibilité.

En créant conjointement un « programme de référence », qui reflète la situation réelle du secteur de l'énergie, les clients pourront découvrir de manière concrète la technologie mise en place, intégrée aux terminaux, aux réseaux ou encore au Cloud. Cette solution est centrée sur les besoins de l'industrie de l'énergie, tels que la connaissance de la situation mais aussi la protection multizone, le soutien de l'acquisition des données et le contrôle de la surveillance native (SCADA) ou encore, la gestion des périphériques à distance.

Ce « programme de référence » permettra notamment au public d'assister à une simulation de cyberattaque déjouée par la solution McAfee Embedded Control et de voir quels seraient les impacts d'une attaque réussie à cause de la mauvaise configuration du système. ■

# Résultats de l'enquête de collecte des indicateurs TIC au titre de l'année 2011

L'enquête annuelle de collecte des indicateurs des technologies de l'information et de la communication auprès des ménages et des entreprises au titre de l'année 2011 a été réalisée entre Janvier et Mars 2012 selon les recommandations internationales et en prenant en considération les spécificités du marché marocain. Les principaux résultats de cette étude se présentent comme suit :

## Équipement et utilisation des TIC par les ménages

### √ Téléphonie Fixe

- 35% de ménages équipés (soit 5 points de moins qu'en 2010) avec 19% de ménages équipés en fixe avec mobilité restreinte contre 18% pour le fixe classique. La baisse de l'équipement des ménages en téléphonie fixe s'explique par le recul du fixe avec mobilité restreinte.

### √ Téléphonie Mobile

- 87% des individus sont équipés en téléphonie mobile (soit une hausse de 4 points par rapport à 2010).
- 17% des individus sont multi-équipés avec pour principale raison la volonté d'optimiser leur facture téléphonique totale.
- Le taux de changement d'opérateur a augmenté de 3 point en 2011 (7% des individus équipés en mobile).
- 12% des individus équipés en mobile disposent de Smartphones dont la majorité appartient à la Classe Socio-professionnelle supérieure.

### √ Ordinateurs

- 39% des ménages sont équipés en ordinateurs (5 points de plus qu'en 2010).
- Le parc estimé pour 2011 est de 3.547.000 unités (contre 3.134.000 en 2010).
- L'ordinateur portable commence à prendre le dessus avec 56% du parc global et le multi-équipement devient un

phénomène marquant (28% des ménages équipés en deux ordinateurs ou plus).

- Le principal frein à l'achat d'un ordinateur en 2011 n'est plus le prix trop élevé, mais le manque de besoin : Le facteur prix est en retrait de 14 points.
- Les intentions d'équipement en ordinateurs en 2012 chez les ménages non équipés sont très fortes (29%).



### √ Internet

- 35% des ménages sont équipés en accès Internet (soit 10 points de plus qu'en 2010).
- En 2011, 30% des ménages ont un accès mobile de type 3G contre 10% qui ont un accès ADSL.
- Le facteur « Prix » était le principal facteur de non-équipement en accès Internet en 2010, mais il perd 10 points en 2011 au profit du facteur « absence d'utilité ».
- Les cybercafés restent le principal lieu de connexion hors domicile avec 22% des connexions, devant le domicile d'un autre particulier à 10%.
- En 2011, le nombre d'internautes a été évalué à 14,9 millions d'utilisateurs.
- En 2011, les internautes ont un usage accru des réseaux sociaux (83% des interviewés) et de la messagerie instantanée (81%) alors que le téléchargement semble être en retrait.

## Équipement et utilisation des TIC par les entreprises :

### √ Téléphonie :

- 99,6% des entreprises sont équipées en téléphonie fixe et 88% en téléphonie mobile.

### √ Ordinateur :

- La totalité des entreprises est équipée en ordinateurs.
- Le ratio nombre d'ordinateurs par employé est de 0,83 (contre 0,57 en 2010).
- Le parc d'ordinateurs est majoritairement composé d'ordinateurs de bureau (79% contre 21% pour les ordinateurs portables).
- Les deux tiers du parc d'ordinateurs a moins de 3 ans.

### √ Internet :

- 90% des entreprises sont connectées à Internet. Parmi ces entreprises, 96% ont un accès ADSL, 45% utilisent l'accès 3G sur téléphone mobile et 42% l'accès 3G sur ordinateur. Les liaisons louées et la fibre optique commencent à émerger (respectivement 12% et 9%).
- 75% des postes de travail sont connectés à Internet (contre 67% en 2010).
- La messagerie, la recherche d'informations commerciales et officielles et les relations avec les organismes gouvernementaux constituent toujours les principaux usages de l'Internet par les entreprises.
- 55% des entreprises connectées à Internet ont un site web (contre 48% en 2010).
- 82% des entreprises ayant un site web possèdent un nom de domaine propre.
- Les entreprises consacrent 8% de leurs budgets à l'investissement dans les TIC et 4% de leurs budgets formation à la formation des employés aux TIC.
- 28% des entreprises connectées à Internet achètent ou effectuent des commandes via Internet (17% en 2010) et 14% vendent leurs produits ou services en ligne (11% en 2010). Les intentions pour 2012 restent fortes. ■

# UTM les appliances de sécurité multifonctions

**L**es "appliances" de sécurité multifonctions regroupent tous les aspects de la sécurité d'une connexion internet dans un seul boîtier, qui se veut simple à administrer. Pléthorique, l'offre cible essentiellement les PME mais monte en gamme.

La sécurité est un véritable casse-tête pour les entreprises qui doivent acquérir différents équipements et logiciels, les faire dialoguer, les mettre à jour et posséder les compétences correspondantes. Or, cet effort est souvent trop important pour les petites et moyennes entreprises.

C'est pour elles que sont nés les "appliances" multifonctions, boîtiers qui prennent en charge les principaux aspects de la sécurité d'un réseau connecté à l'internet. Leur succès est tel que pratiquement tous les constructeurs, voire éditeurs spécialisés dans la sécurité, s'y mettent. Se côtoient ainsi Cisco, Symantec, ISS, SonicWALL, WatchGuard, Netscreen (dans le giron de Juniper), et Fortinet.

## Des boîtiers polyvalents et simples à mettre en oeuvre

Ces produits ont différentes fonctionnalités: firewall, passerelle VPN, prévention et détection d'intrusions, ainsi que filtrage d'URL, antivirus et parfois "anti-spam". Toutefois, ces dernières fonctions sont souvent optionnelles, voire inexistantes. Lorsque ces fonctions sont présentes, les bases de signatures de virus et d'attaques, ainsi que les listes d'URL sont mises à jour automatiquement.

Le matériel prend la forme d'une boîte noire administrable via une interface web, et qui tourne sous un système propriétaire généralement dérivé de Linux.

Pour clore le volet matériel, certains

appliances troquent, pour des raisons de fiabilité, le disque dur contre une mémoire flash. Côté connectivité, ces équipements qui s'insèrent entre le LAN et le WAN n'excèdent pas pour la plupart quatre à huit ports Ethernet, sur lesquels seront reliés des commutateurs de plus grande capacité. Excepté sur les produits d'entrée de gamme, il est possible de définir des politiques de sécurité spécifiques à chaque port, donc des DMZ. D'autre part, SonicWALL et Symantec innovent en lançant des "appliances" intégrant une borne Wi-Fi. Grâce à un chiffrement IP-Sec, le réseau sans fil est alors mieux protégé que via les standards WEP et WPA.

## Pléthorique, l'offre cible essentiellement les PME mais monte en gamme. Une administration pouvant être centralisée

Chaque modèle "d'appliance" est censé protéger un certain nombre de postes de travail – de quelques PC à des dizaines de milliers. Même les grands comptes sont désormais intéressés, car ils y voient un moyen de faire baisser leurs coûts et de faciliter le déploiement en environnement distribué. La capacité annoncée dépend toutefois des fonctions activées, chacune consommant mémoire et puissance.

De la polyvalence de ces "appliances" découlent d'autres avantages. À commencer par l'intégration entre les différentes fonctions. Celles-ci ont besoin d'interagir; la fonction de

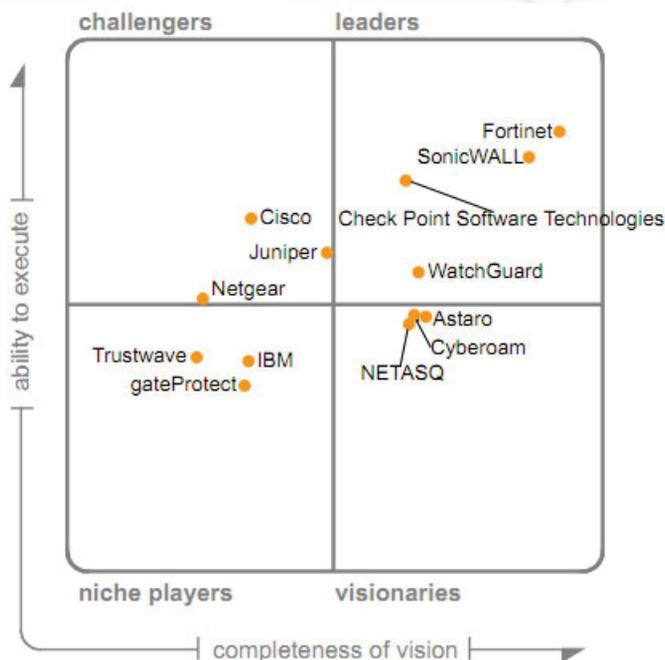
détection d'intrusions doit par exemple pouvoir demander au firewall de bloquer une attaque.

D'autre part, l'administration peut être centralisée, aussi bien fonctionnellement que géographiquement, à partir d'une interface utilisateur unique. Ainsi, une même configuration peut être dupliquée sur des "appliances" déployés sur différents sites.

## Une polyvalence qui a peut-être un revers

Le niveau de sécurité est l'un des arguments avancés contre ces appliances: il est forcément inférieur à celui d'une solution construite avec des briques acquises chez différents spécialistes. Les fournisseurs "d'appliances" multifonctions proposent en effet leurs propres technologies de firewall, de détection d'intrusions et de VPN. Mais ces derniers sont désormais bien standardisés. De plus, pour l'antivirus ou le filtrage d'URL, ces acteurs passent des accords avec des spécialistes.

## Magic quadrant UTM :





## Iomega Personal Cloud

[www.iomega-personal-cloud.com](http://www.iomega-personal-cloud.com)



**A partir de  
3 900 Dirham HT**

# CONNEXION

## FAIRE DU CLOUD COMPUTING UNE REALITÉ



- Technologie révolutionnaire de protection et de partage de données
- Téléchargez et partagez des fichiers entre des ordinateurs PC et Mac lorsque vous êtes en déplacement
- Copiez des fichiers entre des périphériques Iomega, comme s'il s'agissait d'un réseau local
- Invitez jusqu'à 250 membres dans votre Personal Cloud
- Chiffrement et protection par mot de passe inclus pour empêcher l'accès des utilisateurs non autorisés
- Aucun frais mensuel de stockage ou de service après-vente, JAMAIS !
- Inclus sur les nouveaux périphériques de stockage de bureau Iomega Home Media et StorCenter Network
- Accéder à distance à vos fichiers depuis votre iPad® ou votre iPhone® avec Iomega Link

**iomega LINK**

**MEDIA STORE**<sup>™</sup>  
INFORMATIQUE

Disponible chez MEDIA STORE  
Tel: 0212 52 86 55 11 - Email: [mediastore@mediastore.ma](mailto:mediastore@mediastore.ma)

# DLP : Data Loss/Leak Prevention

Le terme Data Loss/Leak Prevention (DLP) fait référence à un ensemble de techniques de protection contre la fuite d'informations.

Le DLP permet de protéger les actifs informationnels de l'entreprise et d'assurer la continuité des activités de l'entreprise en gérant la conformité et les risques, en prévenant les pertes de données et en sécurisant les processus métier.

Les points de fuite potentiels touchent l'ensemble des actifs du système d'information aussi bien en interne que lors d'échanges vers l'extérieur de l'organisation.

## Les techniques DLP peuvent être de plusieurs types :

- Réseau : passerelle d'analyse de trafic (mail, messagerie instantanée, FTP, http et https)
- Au niveau serveur
- Data identification (mots clés, expressions régulières) pour identifier les données sensibles

Une des premières fonctions des produits de DLP (Data Lost/Leak Prevention) est de prévenir la fuite d'information de l'entreprise et, ce, que celle-ci soit intentionnelle ou non.

Ces produits peuvent aussi être utilisés dans le cadre d'audits et / ou d'analyse avec des objectifs métiers pour cartographier les données dites confidentielles au sein du Système d'Information, par exemple pour répondre à des problématiques normatives telles que PCI-DSS (recherche de numéro de carte bleu par exemple).

## Les produits de DLP ne sont pas des produits Plug & Play.

Habitué à vendre de la sécurité "in the box", les intégrateurs de produits de sécurités historiques ont pris le marché du DLP, comme un produit "de plus" à

vendre, avec les mêmes problématiques de déploiement que celle qu'implique la mise en place d'un pare-feu ou d'un antivirus.

La problématique du DLP et de son succès mitigé peut être en (majeure) partie imputable à l'intégrateur.

En effet, le contrôle des données "confidentielles" en mouvement ou stockées au sein du Système d'Information (sur les ressources qui le composent) peut s'avérer très complexe! Ce constat démontre que les produits de DLP ne sont pas des produits Plug & Play.

## L'importance négligée de l'étape préliminaire

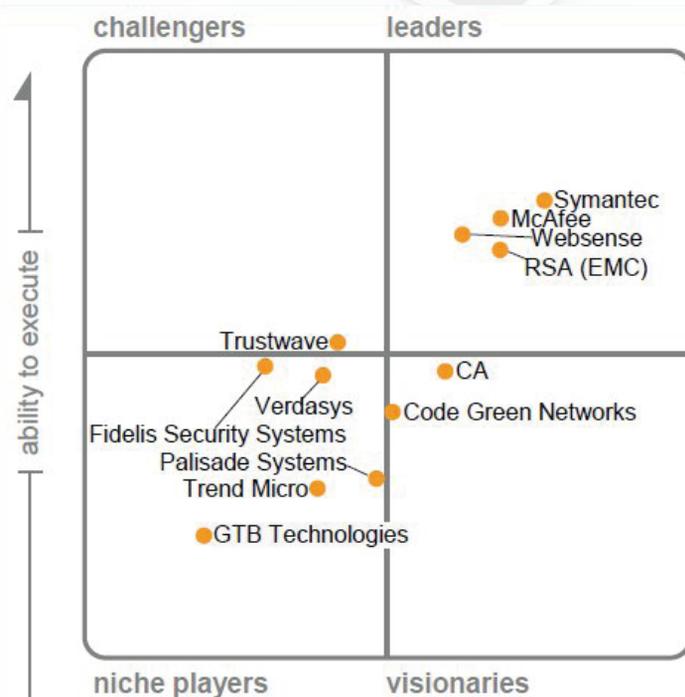
Bien que l'installation d'un produit de DLP dans une problématique d'audit, par exemple, peut rester assez simple. La mise en place d'une politique de DLP pour répondre à une problématique de prévention de fuite d'information confidentielle peut s'avérer très complexe. Non pas en termes d'installation des produits (sur le réseau, les postes de travail ou encore sur les points de sorties Internet (messagerie compris), mais à cause de l'interaction produits / données de l'entreprise.

Cette configuration demande une étape préliminaire à la mise en place des produits qui est, trop souvent négligée: un premier niveau de classification pragmatique des données par les métiers. Il est primordial d'impliquer les métiers dans ce type de projet! Sans cette étape le produit peut s'avérer contreproductif.

## Sélection DLP : Bonnes pratiques de déploiement :

- Le déploiement DLP commence habituellement sur le réseau parce que c'est la façon la plus effective d'un point de vue coût pour obtenir la plus large couverture.
- La surveillance du réseau est non-intrusive et offre une visibilité vers tout système sur le réseau, géré ou non géré, serveur ou poste de travail
- L'ajout d'un agent de point de terminaison (End Point) pour une solution de DLP permet de protéger les données quand elles sont utilisées de façon active.
- Bien que très puissant, il reste problématique à mettre en œuvre. Les agents ne performant que dans la limite des ressources d'un ordinateur standard tout en devant conserver la surveillance du contenu.
- Les organisations commencent généralement par un déploiement sur le réseau et les environnements de stockage et restreignent le transfert de contenu sensible aux périphériques USB non cryptés.

## Magic quadrant for content-aware Data Loss Prevention.



Le DLP nécessite à la fois une approche organisationnelle et technologique. En effet, l'entreprise pour la mettre en place doit identifier précisément par métiers les données sensibles à protéger. Puis on devra classifier les informations en fonction de leurs niveaux de confidentialité. Une fois ce travail effectué, il est aussi important de sensibiliser les utilisateurs, mais aussi de les avertir que certains de leurs mails seront scannés en fonction des mots clés prédéterminés. Il est donc nécessaire de travailler avec les syndicats, etc... pour expliquer et qualifier les procédures. Enfin, on pourra déployer les outils technologiques qui répondront aux besoins de l'entreprise. Les experts préconisent aussi de se préparer à gérer des incidents, ou même une crise, car comme tout le monde le sait, dans le domaine de la sécurité, le 100% est un mirage.

#### À propos de Devoteam

Devoteam est un groupe de conseil en technologies de l'information et de la communication créé en 1995. La combinaison d'une offre de conseil et d'une offre de solutions technologiques permet à Devoteam d'apporter à ses clients un conseil indépendant et des solutions performantes dans l'alignement de l'infrastructure technique de leur système d'information avec leurs objectifs stratégiques.

Devoteam a réalisé, en 2011, un chiffre d'affaires de 528 M€, en hausse de 7% par rapport à 2010 et la marge d'exploitation s'élève à 5,5% du chiffre d'affaires. Le Groupe compte 5.000 collaborateurs dans vingt-quatre pays d'Europe, d'Afrique du Nord et du Moyen-Orient. ■

## Seconde année de hausse consécutive pour les logiciels de gestion des opérations IT



D'après Gartner, les ventes de logiciels de gestion des opérations IT ont rapporté l'an dernier 18,3 milliards de dollars. C'est 8,7 % de mieux qu'en 2010.

Pour la seconde année consécutive, ce marché est orienté à la hausse, mais il reste dominé par cinq acteurs majeurs qui captent plus de 53% des revenus mondiaux.

IBM est le numéro 1 dans ce domaine avec des ventes en hausse de 4,2% et un chiffre d'affaires de 3,2 milliards de dollars.

CA Technologies arrive en seconde position avec 2,2 milliards de dollars de

chiffre d'affaires (+9,4%) et 12,3 % de parts de marché.

Suivent BMC Software avec 1,8 milliard de dollars de chiffre d'affaires (+8,2%), Microsoft avec 1,2 milliard de dollars de chiffre d'affaires (+11,2%) et HP avec 1,18 milliard de dollars de chiffre d'affaires (+3,8).

Gartner note que Microsoft a enregistré la plus forte hausse du marché et que les marchés nord-américains, ouest-européen et asiatiques restent les principales locomotives. Ils représentent à eux trois, 88% du marché.

ITOM Software Vendors, Total Software Revenue, Worldwide, 2010-2011 (Millions of Dollars)

Vendor	2011 Revenue	2011 Market Share (%)	2010 Revenue	2010 Market Share (%)	2010-2011 Growth (%)
IBM	3,256.4	17.8	3,126.5	18.6	4.2
CA Technologies	2,258.1	12.3	2,064.0	12.3	9.4
BMC Software	1,833.0	10.0	1,693.5	10.1	8.2
Microsoft	1,271.9	6.9	1,143.5	6.8	11.2
HP	1,185.4	6.5	1,141.7	6.8	3.8
Others	8,498.1	46.4	7,676.1	45.6	10.7
<b>Total</b>	<b>18,302.9</b>	<b>100.0</b>	<b>16,845.4</b>	<b>100.0</b>	<b>8.7</b>

## Nexans sponsor du Alcatel-Lucent Enterprise Dynamic Tour à Marrakech

Alcatel-Lucent 

 Nexans

**D**urant le Dynamic Tour d'Alcatel-Lucent qui a eu lieu le 20 mai à Abu Dhabi et le 7 juin à Marrakech, Nexans Cabling Solutions a présenté ses solutions en infrastructure réseaux.

Le thème principal de l'édition 2012 était le BYOD «Bring Your Own Device».

L'usage des équipements personnels dans l'univers professionnel, engage les entreprises à repenser leurs réseaux et leurs systèmes IT pour maîtriser l'accès aux diverses plateformes tout en assurant la mobilité et l'efficacité des collaborateurs.

Par conséquent, il faut prévoir des infrastructures réseaux locaux adéquats pour les applications et technologies de demain. Nexans a démontré comment relever certains des grands défis relatifs aux infrastructures IT et relier de façon pertinente les points

suivants et en même temps réduire votre coût total de possession (TCO).

- Créer un environnement qui vous permet d'anticiper facilement l'évolution et l'émergence des technologies que ce soit à court ou long terme ;
- Trouver des chemins de migration qui vous permettent de répondre aux besoins d'augmentation de bande passante ;
- Trouver des moyens d'accroître l'efficacité énergétique, en rendant votre infrastructure IT plus respectueuse de l'environnement ;
- Trouver des moyens pour améliorer la sécurité de votre réseau.

### A propos de Nexans

Inscrivant l'énergie au cœur de son développement, Nexans, expert mondial de l'industrie du câble, propose une large gamme de câbles et solutions de câblages. Le Groupe est un acteur majeur des marchés de transmission et distribution d'énergie, de l'industrie et du bâtiment. Les solutions de Nexans servent de nombreux segments de marché : depuis les réseaux d'énergie et de télécommunication, en passant par

les ressources énergétiques (éoliennes, photovoltaïque, pétrochimie, industries minières...), jusqu'au transport (construction navale, aéronautique, automobile et automatismes, équipements ferroviaires...). Dans le domaine des systèmes de câblages structurés, Nexans Cabling Solutions - filiale du groupe Nexans - propose une gamme complète de produits et services à valeur ajoutée offrant compétitivité et performances aux responsables informatiques et aux installateurs.

En complément des solutions d'infrastructure de câblage LANmark, Nexans est spécialisé dans le développement de solutions intelligentes de gestion d'infrastructure sous la marque LANSense qui inclut la gestion et le contrôle environnemental et le contrôle d'accès. (EMAC).

Nexans offre un choix complet de solutions d'infrastructure LAN à une clientèle mondiale, au travers d'un réseau de bureaux régionaux et d'une équipe de responsables grands comptes.

Pour plus d'informations : [www.nexans.com](http://www.nexans.com) ou [www.nexans.mobi](http://www.nexans.mobi) . ■

SOUS L'EGIDE DU MINISTÈRE DE L'INDUSTRIE, DU COMMERCE ET DES NOUVELLES TECHNOLOGIES

Royaume du Maroc  
Ministère de l'Industrie,  
du Commerce et des  
Nouvelles Technologies



المملكة المغربية  
وزارة الصناعة  
والتجارة  
والتكنولوجيات الحديثة

med-IT

4<sup>ème</sup> SALON INTERNATIONAL  
DES TECHNOLOGIES DE L'INFORMATION

DU 13 AU 15 NOV. 2012



3 JOURS  
au COEUR de  
L'INNOVATION IT

CASABLANCA | OFFICE  
DES CHANGES

# TechnoMagazine

Le Magazine NTIC au Maroc [www.TechnoMag.ma](http://www.TechnoMag.ma)

...les nouveautés NTIC entre vos mains

**Le 1<sup>er</sup> magazine NTIC mensuel gratuit  
au Maroc**

**Magazine  
mensuel  
gratuit**

**Siteweb  
[www.technomag.ma](http://www.technomag.ma)**

**Newsletter  
trois fois par semaine**

*Abonnez-vous et recevez gratuitement  
votre newsletter et votre magazine .*



[www.TechnoMag.ma](http://www.TechnoMag.ma)

Suivez-nous



Pour Toutes informations, contactez-nous: Tél: 0522 47 39 31 e-mail: [contact@technomag.ma](mailto:contact@technomag.ma)

# M. Julien PULVIRENTI



**Julien PULVIRENTI**  
Territory Sales Manager Maghreb

## TM : Parlez-nous de Kaspersky ?

**JP :** Kaspersky Lab est un éditeur international de solutions et de services de sécurité fondé en 1997 qui compte près de 2000 employés à travers le monde, dont plus de 700 chercheurs et développeurs.

En 10 ans, Kaspersky Lab est devenu un leader mondial, présent dans plus de 60 pays. Le laboratoire Kaspersky Lab, parmi les plus réputés au monde, analyse et traite 24h sur 24, 7 jours sur 7 les codes malicieux et développe des antidotes proposés aux utilisateurs via des mises à jour toutes les 45 minutes.

Les solutions de Kaspersky Lab protègent aujourd'hui plus de 300 millions d'utilisateurs à travers le monde.

Kaspersky Lab propose des solutions destinées aux

particuliers mais également aux professionnels.

## TM : Comment peut-on avoir vos produits au Maroc ?

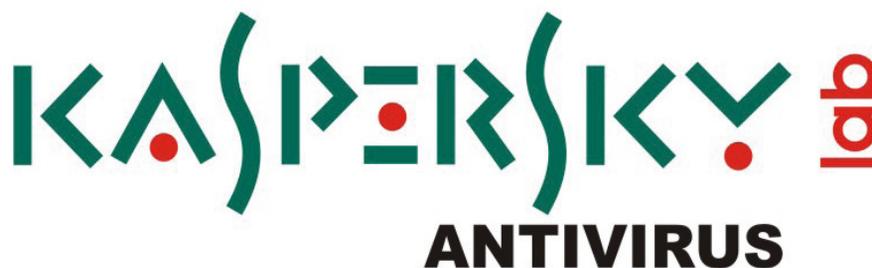
**JP :** Il faut tout d'abord signaler que nous avons 2 types de solutions à proposer, l'une dédiée au grand public et l'autre destinée aux entreprises. C'est pourquoi Kaspersky travaille en permanence à optimiser son réseau de distribution. En effet, les revendeurs peuvent pour certains avoir un profil mixte et s'adresser à la fois aux entreprises et aux particuliers, et d'autres se spécialiser sur un marché. Il faut aussi considérer un business modèle de sous distribution, assez caractéristique du marché du Maghreb. Dans cette démarche Kaspersky a mis en place des

partenariats avec des distributeurs capables de répondre au mieux aux besoins liés à ce marché dynamique. Ainsi les revendeurs marocains peuvent s'adresser à Afinasys (achat de licences ou de boîtes grand public), à Feder (achat de licences ou de boîtes

grand public) ou à Dataco (achat de boîtes grand public) suivant leurs besoins.

## TM : Proposez-vous d'autres solutions que les Antivirus ?

**JP :** Au début de cet entretien nous rappelions que nous avons 20 ans d'existence dans le domaine de l'antivirus. Maintenant, il faut aussi bien se rendre compte qu'Eugene Kaspersky a toujours été visionnaire dans sa façon de « percevoir et d'anticiper » l'évolution de notre marché. Aussi avec de nouvelles tendances fortes comme le cloud computing, la virtualisation, cumulées à une évolution des comportements utilisateurs avec la consommérisation ou encore la mobilité, il fallait s'adapter à cette convergence. C'est pourquoi



vous trouverez dans nos solutions bien plus qu'une simple solution d'antivirus. Ceci reste évidemment le cœur de notre métier, mais nous y avons intégré des fonctionnalités de patch management, de filtrage web et aussi de sécurité autour des architectures virtuelles.

## Territory Sales Manager Maghreb de Kaspersky



**TM :** Quels sont vos points forts par rapport à vos concurrents ?

**JP :** Je crois qu'il faut évaluer un tout : d'abord la technologie. Kaspersky Lab est un leader mondial et reconnu dans son domaine. D'ailleurs dans le dernier rapport du magic quadrant vous nous trouverez positionnés comme tel. Cela est la résultante de l'excellent travail de notre laboratoire en Russie qui reste le plus important au monde. Cela nous permet d'apporter aux responsables de la sécurité ce qu'ils recherchent, à savoir un produit fiable, complet, polyvalent et surtout administrable via une console qui conjugue efficacité et simplicité permettant ainsi une optimisation des coûts. Ensuite, je dis toujours qu'il y a le « système Kaspersky ». En effet, rien ne sert d'avoir une haute technologie si les clients ne peuvent en profiter. Nous sommes exigeants aussi sur notre réseau de distribution. Il est primordial que nous ayons des distributeurs et revendeurs sur place. La

proximité est un point essentiel: le client comprend que dans notre secteur le risque zéro n'existe pas, par contre nous devons tout faire pour que le risque zéro de se sentir seul lorsqu'il a besoin d'accompagnement ou de support n'arrive pas. Nos partenaires et distributeurs certifiés sont là pour ça, et mon rôle en tant que Territory Sales Manager Maghreb est de veiller à ce qu'aucun élément ne puisse venir perturber les bons rouages de ce service que nous devons fournir à nos clients. Par ailleurs, nous savons rester à l'écoute de nos partenaires et j'ai le plaisir de vous annoncer la prochaine disponibilité de notre offre Kaspersky Security for Small Office pour protéger les entreprises jusqu'à 25 postes. Cette offre répond à une demande de nos partenaires d'une solution simple à déployer et à gérer sur cette cible de TPE et PME.

**TM :** Comment voyez-vous le marché des antivirus au Maroc ?

**JP :** Il est indéniable que ce marché est dynamique. Je suis très sensible au fait que les gens, professionnels ou particuliers sont très attirés par le monde des nouvelles technologies, et donc, très au fait de ce qu'il faut faire en matière de sécurité. Néanmoins, un élément important à prendre en compte est le côté « culturel » du piratage. Cependant, grâce au travail cumulé de plusieurs acteurs

de la sécurité, il y a une vraie prise de conscience de l'importance de s'équiper en produits officiels. Ceci laisse augurer de belles perspectives d'évolution !

Par ailleurs, dans le monde de l'entreprise, le taux d'équipement est aujourd'hui très bon, il faut donc fidéliser les clients et leur apporter les solutions adaptées à l'évolution de leurs contraintes et besoins.

**TM :** Avez-vous des chiffres et des statistiques concernant le marché de la sécurité au Maroc ?

**JP :** D'après IDC, lors d'une conférence sur la sécurité informatique (Madame Ouafa Khatir, responsable locale d'IDC), le marché de la sécurité des technologies de l'information au Maroc a représenté en 2010, un investissement de 9,7 millions de dollars. 64% concerne la sécurité de contenu et les logiciels de gestion des menaces (sécurité réseau, pare feu, anti virus, filtrage du contenu). L'authentification des utilisateurs (mots de passe) représente 21% et la gestion des vulnérabilités 14.1%. Ces chiffres illustrent ainsi comment notre gamme de solutions nous permet d'apporter des réponses aux principales préoccupations des entreprises marocaines. ■

# Le lancement de l'IPv6 révèle des défis de sécurité

Il ne fait aucun doute que le lancement mondial imminent du protocole IPv6 le 6 Juin 2012 annonce une nouvelle ère de l'infrastructure Internet dans le monde entier, à la fois en termes d'évolution et d'adoption généralisée.

Le monde a déjà eu un avant-goût du nouveau protocole en Juin dernier, lors de la Journée Mondiale IPv6. Mené par l'Internet Society, plus de 1 000 sites Internet, entreprises high-tech et FAI ont été encouragés à passer collectivement à l'IPv6 durant une période de 24 heures pour "tester" le protocole et essayer d'anticiper les problèmes techniques qui pourraient se produire lors du lancement officiel.

Le 6 Juin 2012, les principales organisations high-tech et leaders du Web tels que Google, Facebook et Yahoo!, entre autres, basculeront vers le nouveau protocole Internet lors du lancement mondial officiel.

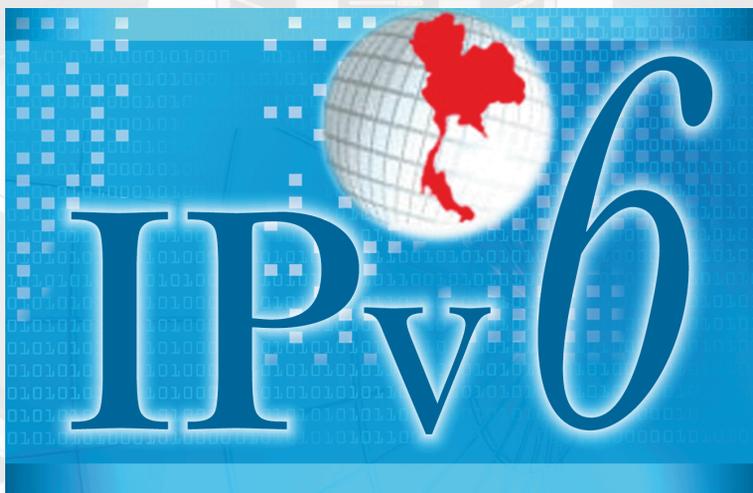
Et la transition devient de plus en plus nécessaire. Le protocole actuel IPv4, qui supporte environ 3,7 milliards d'adresses, a simplement épuisé le stock d'adresses disponibles, en partie du fait de l'explosion des appareils mobiles. Mais l'IPv6, de son côté, a une capacité illimitée d'adresses ce qui lui permet de s'adapter à une infrastructure mobile et Internet mondiale en pleine croissance.

Cependant, avec le lancement imminent du protocole mondial IPv6, les chercheurs et professionnels de l'IT anticipent certains défis, en particulier en matière de sécurité.

L'aspect novateur et le manque de connaissances relatifs au protocole IPv6 feront qu'il y aura forcément des erreurs de configuration, des problèmes de compatibilité et autres maladrotes d'implémentation. Il n'existe pas les

connaissances institutionnelles sur l'IPv6 que l'on a sur l'IPv4, qui a été utilisé depuis des décennies et offre une vaste base de connaissances.

Mais peut être que le plus important défi en matière de sécurité est que de nombreux appareils de sécurité réseau sont capables de transférer le trafic IPv6, mais pas de l'inspecter. Et, comme l'IPv6 est activé par défaut sur de nombreuses plateformes réseaux actuelles – tel que Windows 7 – ces systèmes sont déjà installés sur le réseau.



La plupart des systèmes qui n'ont pas l'IPv6 activé ont la capacité de contourner ce problème en encapsulant les paquets IPv6 d'en-têtes IPv4. Ils lisent l'en-tête, mais ne peuvent pas lire le contenu du paquet en lui-même. Ils ne peuvent donc pas faire l'inspection approfondie habituelle des paquets, et transfèrent donc juste les paquets. C'est seulement quand ils ont une implémentation dual stack, qu'ils peuvent autoriser les fonctions de sécurité réseau à simultanément traiter et inspecter les paquets provenant à la fois des protocoles IPv4 et IPv6.

Plusieurs constructeurs de sécurité offrent cette fonctionnalité – mais pas tous – et c'est justement l'un des risques auxquels sont confrontés les professionnels de la sécurité réseau aujourd'hui. Ils doivent s'assurer que leurs produits de sécurité peuvent inspecter

le trafic IPv6. S'ils peuvent seulement transférer le trafic IPv6, ces produits pourraient également transférer le contenu malveillant.

Même avec une implémentation dual stack, les organisations ont néanmoins besoin de vérifier si elles ont les mêmes fonctionnalités de sécurité activées pour le protocole IPv4 que pour l'IPv6. Dans le cas contraire, les appareils de sécurité réseau sont susceptibles de laisser passer des éléments critiques du trafic malveillant qui pourraient potentiellement compromettre le réseau.

Certaines des politiques et technologies sur lesquelles vous comptez peuvent uniquement fonctionner en IPv4 et non en IPv6, et créent ainsi les déficits de votre couverture de sécurité. Cependant, mettre à jour l'infrastructure de sécurité réseau pour permettre le transfert à l'IPv6 n'est pas un projet simple et prendra probablement des années pour être complètement abouti. C'est pourquoi de

nombreuses organisations, faisant face à des mises à jour matérielles qui sont potentiellement longues et onéreuses, n'ont pas prévues d'adopter l'IPv6 de si tôt.

Pourtant, les entreprises ne vont pas pouvoir éviter l'IPv6 encore trop longtemps. Suite au lancement du 5 Juin, beaucoup plus de trafic IPv6 atteindra leurs réseaux. Lorsque l'IPv6 représentera 5 à 10 pourcents de vos données – plutôt qu'une fraction de pourcent comme à l'heure actuelle – éviter les mises à jour nécessaires va devenir beaucoup plus difficile à justifier. Les DSI vont donc devoir se pencher sur ce problème rapidement. ■

# E-commerce : quelles solutions pour lutter contre la fraude en ligne ?

Pour les e-commerçants et les professionnels du paiement, la lutte contre la fraude en ligne est un combat permanent, dans lequel le risque zéro n'existe pas. Quels sont les secteurs les plus touchés ? A partir de quel taux de fraude faut-il mettre en place des dispositifs de lutte contre la fraude ? Comment remédier au fait que les fraudeurs sont créatifs et trouvent constamment de nouveaux moyens pour contrer les parades ?

## Evaluer les risques de fraude

Bien que la fraude en ligne soit répandue, elle ne touche pas toutes les entreprises avec la même intensité. La première étape, pour le marchand, va donc consister en une auto-évaluation des risques encourus, qui dépendent de plusieurs facteurs. Les principales questions à se poser en matière d'identification des risques sont les suivantes : mon secteur d'activité est-il plus particulièrement touché par la fraude ? Mes produits ou services peuvent-ils être revendus facilement au marché noir ? Quelle est la valeur de mon panier moyen ?

Si les secteurs du tourisme, de la distribution de produits high-tech ou le luxe sont connus pour être plus touchés par la fraude, les autres secteurs d'activité ne sont pas forcément épargnés. Par exemple, les contenus digitaux (billets de spectacles ou places de concert dématérialisés achetés à la dernière minute, sonneries de téléphone, musique, vidéo, etc.) sont également la cible des fraudeurs car la livraison est immédiate. En outre, un commerçant qui vend à l'international sera naturellement plus exposé qu'un marchand qui limite sa zone de livraison à son strict territoire national.

Pour mieux évaluer les risques qu'il encourt, le e-commerçant pourra se renseigner auprès de son opérateur de paiement, ou des organisations professionnelles du e-commerce.

## Calculer le ratio risques / coût

Une fois les risques évalués, le marchand doit ensuite se poser la question du coût d'un développement interne d'un outil de lutte contre la fraude, ou de la mise en place d'une solution du marché. S'équiper n'est valable qu'à la condition que le coût de la solution anti-fraude soit inférieur au coût de la fraude elle-même. Néanmoins, cet argument est à tempérer, car des éléments extérieurs sont

à prendre en compte : les marchands qui connaissent des taux de fraude trop élevés (au-delà de 0,5-0,6%) reçoivent des injonctions de la part des fournisseurs de solutions de e-paiement de prendre des mesures, sous peine de se voir retirer leur licence. Or, et notamment au Maroc, il est difficile, voire impossible de ne pas proposer la carte de paiement bancaire, celle-ci étant le moyen de paiement privilégié pour acheter sur Internet...

## Mettre en œuvre quelques règles simples

Le risque zéro n'existant pas en matière de fraude en ligne, tout l'enjeu va être de rester sous un seuil « tolérable », aux alentours de 0,1-0,2%. Quelques règles simples peuvent suffire pour faire baisser le taux de fraude. La mise en place de règles simples (blocage d'une carte au-delà d'un certain montant ou nombre d'achats successifs réalisés avec une même carte, d'une adresse IP, d'un e-mail, etc.) et la création de listes blanches ou noires, par exemple. Ou, sur un plan géographique, la mise en œuvre d'une règle permettant de refuser systématiquement des paiements en provenance de l'étranger, quand le e-commerçant ne livre qu'au Maroc...



La mise en place de 3D Secure est un autre axe de réflexion. Certes, ce mécanisme rallonge le processus de paiement, en ajoutant une étape au processus de paiement (saisie de la date de naissance ou d'un code à usage unique envoyé par SMS), mais il permet de limiter le risque de fraudes liées aux tentatives d'usurpation d'identité. Pour rester à un taux de fraude tolérable.

Enfin, d'autres outils existent, tels que des bases de données liées aux fraudes et tentatives de fraudes sur Internet.

## Lutte contre la fraude : un métier à part entière

En règle générale, la meilleure solution pour faire baisser son taux de fraude est la combinaison de plusieurs règles et/ou outils, sans pour autant tomber dans l'excès de zèle et risquer de bloquer des transactions légitimes, ou tout simplement décourager les acheteurs...

Pour trouver le bon équilibre, ou quand le risque a d'emblée été évalué comme très fort, un commerçant ne devra pas hésiter à s'entourer d'experts. Après tout, son métier consiste à vendre. Pas à gérer des paiements, et encore moins à lutter contre la fraude...

En la matière, deux solutions s'offrent aujourd'hui à lui : adjoindre à son prestataire de paiement des services de sécurité complémentaires. Ou opter pour une offre intégrée, combinant les deux.

## Faire évoluer ses outils et sa stratégie de protection en permanence

Quelle que soit la solution retenue, une phase de paramétrage sera nécessaire pour prendre en compte les spécificités de chaque marchand, afin de ne pas bloquer des commandes qui n'ont rien de frauduleux. Seuls des experts de la lutte anti-fraude sont capables de procéder à des réglages fins, basés sur les retours d'expérience acquis auprès de leurs clients ; et surtout de faire évoluer la stratégie de protection en permanence, pour contrecarrer les techniques et méthodes toujours plus créatives des fraudeurs. La lutte contre la fraude sur Internet est en effet très similaire à celle contre les virus informatiques, s'apparentant à un cercle sans fin. Ainsi, dès qu'un nouveau virus est identifié, les éditeurs de solutions antivirus l'intègrent à leur base de données afin de protéger leurs clients de cette nouvelle menace. C'est exactement le même principe avec les

outils de protection contre la fraude en ligne... A la différence d'outils développés en interne, les solutions proposées par des fournisseurs spécialisés s'avèrent être plus pérennes : ces tiers de confiance disposent en effet d'une cellule de R&D, dont la mission quotidienne est d'anticiper les tendances et faire évoluer leurs outils. La plupart d'entre eux s'orientent d'ailleurs actuellement vers la détection des comportements à risque par l'empreinte numérique, c'est-à-dire l'identification du terminal, ordinateur, tablette ou smartphone, ayant servi à passer commande... ■

# Les Advanced Evasion Techniques ou AET

Les Techniques d'Évasion Avancées (AET) sont des méthodes évoluées et constituent un nouveau défi pour les systèmes de sécurité réseau. Contrairement aux moyens de contournement connus, les AET combinent et modifient des méthodes afin de déguiser une attaque ou un code malveillant. Ainsi elles infiltrent un réseau sans être détectées par les systèmes de sécurité en place. Le risque particulier associé aux AET est le nombre presque illimité d'options de combinaison qui peuvent s'effectuer. Les estimations actuelles atteignent 2250 variantes d'AET, qui vont servir aux pirates informatiques pour déguiser une attaque. Des mécanismes de protection courants (système de prévention d'intrusion ou pare-feu) ne gèrent pas ces techniques. Il n'existe aucune protection complète contre les AET, néanmoins il est possible de sécuriser des réseaux par des méthodes de prévention.

Pour contourner un système protégé les cyber-pirates déguisent ou modifient des logiciels malveillants et les dirigent, inaperçus, vers des réseaux. Dans le cas de contournements simples et des AET, le protocole TCP/IP, utilisé sur Internet et une majorité de réseaux informatiques, joue un rôle central. Il refait appel à la norme IP RFC 791 et définit un mode de réception ouvert tandis que le mode envoi reste conventionnel. En général seuls des paquets de données sans erreur peuvent être envoyés, et le système accepte tous les paquets de données entrants qui peuvent être interprétés en bout de chaîne. Des paquets de données entrants peuvent disposer de formats différents, mais ils sont toujours interprétés de la même manière. Cette approche ouverte, basée sur la notion que l'interaction entre des systèmes différents doit être aussi fiable que possible, ouvre la porte aux attaques et/ou les techniques déployées pour les déguiser.

Les différents systèmes d'exploitation et applications ne se comportent pas de la même manière en recevant des



paquets de données, et il peut arriver qu'un IPS (Intrusion Prevention System) ne détecte pas le contexte original du paquet et par conséquent, interprète le flux de données différemment de l'hôte cible. On parle dans ce cas de «désynchronisation de statut». C'est le point de départ pour des techniques de contournement, qui utilisent ce contexte pour créer les paquets de données qui apparaissent normaux et sécurisés. Ces paquets ne sont identifiés comme des attaques que quand ils sont interprétés par le système final, c'est-à-dire, quand le code malveillant est déjà installé dans le réseau.

## Quel risque particulier associe-t-on aux AET ?

Jusque très récemment, on connaissait quelques techniques de contournement, qui étaient correctement gérés par les solutions de sécurité. Mais depuis la découverte de Techniques Avancées, il est évident que davantage de techniques peuvent être utilisées pour contourner des systèmes IPS. Les AET exploitent des vulnérabilités dans des protocoles et les faibles barrières de sécurité de la communication réseau. Tout comme les méthodes conventionnelles,

elles commencent par "le statut désynchronisé" décrit plus haut. Or les AET font preuve de plus de finesse encore - elles varient constamment, combinent les techniques de déguisement et visent différentes couches du réseau.

## Les nouveaux champs d'attaque

Les tests de départ ont identifié la possibilité d'attaques AET au niveau de l'IP, du transport (TCP, UDP) et des protocoles de couche applicatives (SMB et RPC). Le phénomène a donc été identifié comme une menace interne. Des AET intervenant au niveau d'autres protocoles, comme IPV4, IPV6, TCP et HTTP, ont aussi fait surface en automne 2011. Si les AET visent la couche de protocole HTTP (le Port 80 et donc l'Internet), elles peuvent aussi tromper les pare-feux et faire passer des logiciels malveillants dans le réseau via le trafic Web. Cela signifie que les cyber-pirates peuvent utiliser les AET pour atteindre les environnements Cloud tout comme des applications et données Web. Le protocole IPV6 offre aux AET de nouvelles façons de déguiser des attaques protocolaires ou agissant au niveau du transport. En raison de la compatibilité exigée avec IPV4, les systèmes doivent

faire preuve d'une plus grande tolérance lors de l'interprétation de paquets de données entrants. Cela augmente la dérive pour les AET lorsqu'il s'agit de déguiser des codes malveillants. Un facteur aggravant est notre manque d'expérience et de recul par rapport à l'IPv6.

A ce jour plus de 300 AET différents ont été identifiés. Ce n'est qu'une goutte d'eau! On peut estimer les combinaisons potentielles aujourd'hui à 2250. Voici donc le défi auquel les systèmes de sécurité sont confrontés à présent. La protection fiable contre des attaques réseau déguisées par le biais des AET implique que les IPS doivent connaître et intégrer toutes les variantes AET utilisables par un système cible pour rassembler des fragments de données.

### Comment se protéger contre les AET?

Les dispositifs d'inspection de flux fonctionnent avec des analyses de protocole et détections de signature. Cela signifie qu'un système IPS doit déjà être familier avec un modèle d'attaque pour pouvoir l'éviter. Vu le nombre potentiel des AET la tâche est très difficile. Il est vrai que les méthodes de détection correspondantes sont généralement ajoutées aux dispositifs quelques jours après la découverte de nouvelles menaces. En outre, il existe des fonctions analytiques qui détectent et bloquent des codes malveillants comparables à ceux qui sont déjà connus. Or, il suffit parfois d'un changement minimal dans le nombre d'octets pour que la variante AET ne ressemble à aucune des attaques répertoriées dans le système IPS. En conséquence, le système de sécurité ne reconnaît pas le code malveillant crypté avec l'AET et le laisse entrer dans le réseau sans blocage. L'attaquant peut alors librement se déplacer dans le système pour chercher

une zone de faiblesse ou un serveur non-patché.

Les IPS doivent donc être à même de gérer plus d'éléments que les simples caractéristiques des codes-menaces pour décerner les attaques AET. Les applications de sécurité qui comparent des signatures d'attaque reçues par l'hôte cible avec des signatures déjà connues ne peuvent pas prendre en compte chaque paquet du trafic réseau. Il ne suffit pas de trier tous les paquets dans l'ordre et rassembler tous les fragments. C'est pourquoi les fonctions d'IPS classiques généralement utilisées pour protéger contre des exploits - comme la prise des empreintes digitales ou la détection à base de signature - ne protègent pas contre les AET.

toutes les couches pertinentes pour chaque connexion. Le risque que les paquets de données ne se comportant pas selon les règles RFC 791 puissent contourner des systèmes de sécurité sans détection est réduit.

Les réseaux devraient aussi être protégés avec des systèmes de sécurité flexibles à base de logiciel. Ils n'offrent pas la protection 100 % garantie contre les AET mais peuvent être ajustés aux modèles d'attaque changeants plus facilement et rapidement que des solutions matérielles. Contrairement aux solutions matérielles, les solutions logicielles tiennent compte de la mise en œuvre immédiate des patch de sécurité et des mises à jour. La gestion centralisée est également un atout pour le traitement efficace des AET.



### Quel est l'objectif des AET à présent ?

On ne peut pas mesurer avec exactitude l'utilisation actuelle des AET. Ne laissant pas de trace, ces attaques sont découvertes quand elles sont déjà entrées dans le réseau. Mais alors il n'est plus possible de dire quelle technique a été utilisée pour permettre au code malveillant de contourner les systèmes de sécurité. Des recherches actuelles indiquent que certaines AET sont relativement faciles à manipuler, et on peut supposer que les

### La Normalisation

Des options complémentaires sont nécessaires pour inspecter le flux de données, tels que des paquets de données non reçus en bout de système ou les protocoles qui peuvent être décryptés différemment. Ces contrôles supplémentaires peuvent être mis en œuvre avec un mécanisme appelé la normalisation. Les instruments de sécurité qui sont capables de mettre en œuvre des processus complets de normalisation interprètent des paquets de données et les rassemblent comme le système final. Ils prennent en compte

pirates informatiques les utilisent déjà. D'autres sont très complexes et leur utilisation exige des ressources financières considérables ainsi que le savoir-faire technique. De telles ressources et savoir-faire sont du ressort des cybercriminels organisés agissant selon des intérêts économiques ou politiques. On en conclut que les attaques déguisées par les AET constituent une menace pour les données sensibles de grandes sociétés, des agences gouvernementales ou des banques. ■

# Flame serait-il le maliciel le plus complexe depuis Stuxnet et Duqu ?

L'équipe de chercheurs du Security Response de Symantec procède à l'analyse d'une menace aussi sophistiquée et discrète que l'étaient Stuxnet et Duqu : W32.Flamer. Cette analyse a jusqu'à présent révélé que le maliciel a été conçu dans le but d'obtenir des informations de la part des systèmes infectés, qui se trouvent principalement au Moyen-Orient. Comme pour Stuxnet et Duqu, le code de cette nouvelle menace n'a pas été écrit par un individu isolé mais par un groupe de spécialistes organisé, financé et dirigé. Le code comporte de multiples références à la chaîne «FLAME», ce qui peut donner une indication soit sur les instances d'attaque via différentes parties du code, soit sur le nom du projet de développement du maliciel.

Ce maliciel, particulièrement discret, est en activité depuis au moins 2 ans et a la capacité de voler des documents, faire des copies-écran des utilisateurs de la machine infectée, de se propager via les disques connectés en USB, de désactiver les solutions des éditeurs de sécurité et, sous certaines conditions, se développer sur d'autres systèmes. Cette menace a également la capacité d'utiliser plusieurs vulnérabilités connues et corrigées de Microsoft Windows pour se propager sur un réseau.

Les premières analyses de localisation montrent que Flamer se trouvent principalement en Cisjordanie, en Hongrie, en Iran et au Liban. D'autres cibles se trouvent en Russie, en Autriche, à Hong Kong et aux Emirats Arabes Unis. Les secteurs d'activité des individus ciblés sont pour le moment indéterminés. Cependant, les premières analyses du maliciel montrent que les victimes n'ont pas toutes été ciblées pour la même raison. Nombre d'entre elles semblent être ciblées pour leurs activités personnelles plutôt que pour celles de la société qui les emploie. Il est également intéressant de noter que, au-delà de sociétés spécifiques ciblées, de nombreux systèmes attaqués sont des ordinateurs utilisés à domicile et connectés à Internet.

## Win32.Flame également détecté par Kaspersky

Le malware a également été identifié

par les experts de Kaspersky Lab au cours d'une enquête déclenchée par l'Union internationale des télécommunications (UIT). Le programme malveillant, détecté sous la dénomination Worm.Win32.Flame par les solutions de sécurité de Kaspersky Lab, est conçu pour se livrer à des activités de cyberespionnage. Il peut ainsi dérober des informations, notamment (mais pas uniquement) celles affichées sur des écrans d'ordinateurs ou concernant les systèmes ciblés, les fichiers stockés, les listes de contacts, voire les conversations audio.

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD"))())
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())
  if not __LIB_FLAME_PROPS_LOADED__ then
    LIB_FLAME_PROPS_LOADED__ = true
    Flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK"
    flame_props.INTERNET_CHECK_KEY = "CONNECTION.TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE"
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getKeyId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
      end
    end
```

Des études indépendantes ont été lancées par l'UIT et Kaspersky Lab après une série d'incidents relatifs à un autre malware destructeur, encore inconnu (nom de code Wiper), responsable de l'effacement de données dans un certain nombre d'ordinateurs en Asie occidentale. Ce malware spécifique reste à identifier mais, en analysant ces incidents, les experts de Kaspersky Lab, en coordination avec l'UIT, ont rencontré le nouveau type de code maléfisant. Les premiers résultats indiquent que celui-ci se trouve « dans la nature » depuis plus de deux ans, plus précisément depuis mars 2010. En raison de son extrême complexité ainsi que du caractère ciblé de ses attaques, aucun logiciel de sécurité ne l'avait détecté jusque-là.

Bien que ses caractéristiques diffèrent de celles d'autres cyberarmes notoires découvertes précédemment telles que Duqu et Stuxnet, la répartition géographique des attaques, l'utilisation de vulnérabilités particulières dans les logiciels et le fait que seuls certains ordinateurs soient ciblés constituent autant de signes que Flame appartient à cette même catégorie des «super-cyberarmes».

« Le risque d'une cyberguerre représente l'une des menaces les plus sérieuses dans le domaine de la sécurité informatique depuis plusieurs années déjà. Stuxnet et Duqu faisaient partie d'une même série d'attaques, qui a fait naître les craintes d'un cyberconflit mondial, commente Eugene Kaspersky, CEO et cofondateur de Kaspersky Lab. Le malware Flame paraît correspondre à une autre phase de cette guerre et il faut avoir conscience que de telles cyberarmes peuvent être facilement dirigées contre n'importe quel pays. A la différence des dispositifs d'armements conventionnels, ce sont les nations les plus développées qui sont en fait les plus vulnérables. »

Flame paraît avoir pour principal objectif le cyberespionnage, par le vol d'informations sur les machines infectées. Ces informations sont ensuite transmises à un réseau de serveurs de commande et de contrôle éparpillés à travers le monde. Il peut s'agir aussi bien de documents, de copies d'écrans, d'enregistrements audio que de trafic intercepté, ce qui fait de ce kit d'outils d'attaque l'un des plus évolués et complets jamais découverts. Le vecteur exact d'infection n'est pas encore déterminé mais il est d'ores et déjà clair que Flame a la possibilité de se répliquer via un réseau local par plusieurs méthodes, parmi lesquelles la même vulnérabilité d'imprimante et méthode d'infection USB exploitée par Stuxnet.

Les experts de Kaspersky Lab mènent à l'heure actuelle une analyse plus approfondie de Flame. Dans les jours à venir, une série de billets de blog fournira davantage de détails sur la nouvelle menace. Pour ce que l'on en sait, elle se compose de divers modules représentant au total plusieurs mégaoctets de code exécutable, soit une envergure environ 20 fois supérieure à celle de Stuxnet. L'analyse de cette cyberarme va par conséquent mobiliser une importante équipe d'experts chevronnés de la sécurité et de spécialistes de la rétro-ingénierie, s'appuyant sur une vaste expérience de la cyberdéfense.

L'UIT utilisera le réseau UIT-IMPACT, regroupant 142 pays et plusieurs acteurs du secteur, dont Kaspersky Lab, pour ale ■

# Gestion Globale des Risques



Face à un environnement de plus en plus concurrentiel, les organismes privés et publics ont besoin d'optimiser leurs processus de gouvernance et de maîtrise des risques. Nous assistons, par conséquent, à une forte demande du marché sur les outils de risque. Ci-dessous, on vous propose 10 bonnes pratiques pour maîtriser la gestion de l'ensemble des risques dans entreprise.

## 1 - La Direction Générale, tu impliqueras

Sans son soutien et ses directives pour l'ensemble des départements métiers, support et pilotage, votre projet risque de s'enlisier.

## 2 - La stratégie de gestion des risques, tu formaliseras

Il est important de définir la politique interne de gestion des risques avec des objectifs, un périmètre, une organisation, un processus, des acteurs et des responsabilités (RACI).

## 3 - Le métier, tu associeras en amont des projets

Les directions métier devront aussi être impliquées très en amont dans le projet afin qu'elles se l'approprient. Ces

dernières sont les mieux placées pour identifier, analyser et évaluer les risques auxquels elles sont exposées dans le cadre de leur activité.

## 4 - Des référentiels et normes, tu t'inspireras

La gestion des risques étant mature, les normes (ISO 31000, ...), le référentiel (COBIT 4 : Control Objectives for Information and related Technology) est de plus en plus partagé par l'ensemble des acteurs et permet une transparence accrue auprès de l'ensemble des ayants droits.

## 5 - Des bénéfices du projet, tu feras la promotion

Suite à la cartographie des risques, les entités auditées sont crédibles pour demander des budgets et faire avancer leurs plans d'actions. Vous souhaitez un plan d'actions : faites une cartographie des risques !

## 6 - De manière précise, tu communiqueras

Les incidents évités, les plans d'actions achevés, les risques maîtrisés, les gains apportés doivent être communiqués à l'ensemble des acteurs grâce à des tableaux de bord dynamiques.

La diminution du risque avéré est le premier indicateur clé de calcul d'un ROI sur un projet de gestion des risques. La réalité des incidents avérés permet de challenger la vision prospective de la cartographie des risques.

## 7 - Les entités, tu challengeras

En comparant les cartographies des risques de différentes entités, par un benchmarking des actions de maîtrise entre entités, le risk manager saura être pertinent pour apporter sa propre analyse du risque à chaque correspondant.

## 8 - Les régulateurs, tu choieras

Les lettres de suite et les recommandations des différents régulateurs doivent être finement gérés afin de pouvoir répondre avec aisance aux différents audits sur place et audits sur pièces.

## 9 - Un outil, tu déploieras et interfaceras

Une stratégie de gestion des risques ne peut se faire à la main. La plupart des contrôles manuels peuvent être automatisés. Une solution de gestion des risques est indispensable pour industrialiser les workflow de collecte des données et la production de tableaux de bord pertinents en temps réel pour faire agir l'ensemble des acteurs.

Les données collectées sont généralement déjà existantes soit au niveau du SI, soit sur Internet. La collecte automatique de l'ensemble des indicateurs clé de risque, black list, données de marché, doivent être intégrés automatiquement dans la solution globale de gestion des risques.

## 10 - Des questions, tu renouvelleras

L'écosystème de l'entreprise étant en mouvance perpétuelle, un processus de cartographie des risques à peine finalisé sera remis en fonction d'événements endogènes / exogènes à l'entreprise. ■

# Données à caractère personnel : Quels enjeux et comment se préparer à la loi 09-08 ?



Assemblée Générale Ordinaire Elective du 23 février 2012

## Qui sommes-nous ?

L'Association des Utilisateurs des Systèmes d'Information au Maroc -AUSIM- est une association à but non lucratif créée en 1993. Elle compte parmi ses adhérents de nombreuses structures (Offices, Banques, Assurances, Entreprises Industrielles, ...) qui jouent un rôle de leadership sur le plan organisationnel et managérial au Maroc.

Grâce aux efforts des fondateurs et des différentes équipes qui se sont succédées pour diriger l'Association depuis sa création en 1993, l'AUSIM a gagné son pari d'être considérée comme l'association de référence dans les domaines des Systèmes d'Information au Maroc.

## Nos objectifs

L'AUSIM a pris les devants pour démontrer sa volonté de contribuer à la promotion des systèmes d'information au Maroc tout en s'associant aux autres acteurs du secteur, et s'est donné pour objectifs :

- La promotion de l'usage des Systèmes d'Information au profit de la création de valeur ;
- La contribution à la protection des intérêts de ses adhérents ;
- Le renforcement des liens qui l'unissent aux associations similaires au Maroc et à l'étranger ;
- La diffusion entre les membres des connaissances et des informations relatives aux systèmes d'information ;
- La participation aux grandes réflexions et réformes nationales sur le sujet.

## Nos valeurs

La vision de l'AUSIM est de montrer la voie et jouer le rôle de locomotive pour accélérer la diffusion de l'usage des Systèmes d'Information au Maroc.

### 3 valeurs guident notre action



Constituant de véritables leviers de développement économique et humain, les technologies de l'information jouent un rôle central et déterminant. Ainsi, pour les années à venir, l'enjeu est non seulement de pérenniser les avancées déjà réalisées, mais surtout de permettre une intégration amplifiée et largement diffusée des TI au niveau de l'ensemble des acteurs de la société : État, administrations, entreprises et citoyens.

Pour ce faire, l'instauration d'une stratégie de confiance numérique s'avère fondamentale et devrait assurer au mieux la protection de la vie privée des citoyens. L'actualité mondiale récente l'atteste : il s'agit d'une préoccupation croissante à la fois pour le citoyen, qui entend bénéficier pleinement du potentiel des nouvelles technologies tout en maîtrisant les usages, et pour les investisseurs, aussi bien

privés qu'étatiques, qui n'hésitent plus à en faire une condition décisive avant tout engagement de capitaux.

C'est un défi que le Royaume entend aujourd'hui relever, en se dotant de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Tous les organismes marocains doivent à présent s'y conformer.

Nous le savons : ces nouvelles exigences suscitent de nombreuses interrogations quant à leur champ d'application, leurs implications concrètes, ou encore la démarche à adopter pour y répondre.

En tant que promoteur de l'usage des technologies de l'information au Maroc et dans le cadre de ses missions d'animation du partage de connaissances entre ses membres, l'AUSIM, l'Association des Utilisateurs des Systèmes d'Information au Maroc, souhaite s'engager fortement aux côtés des organismes marocains sur ce sujet.

Ainsi, l'AUSIM a associé à ses efforts Solucom, cabinet de conseil en management & IT, qui dispose de retours d'expériences riches en matière de mise en conformité, acquis auprès de grandes organisations françaises et internationales soumises à des législations équivalentes. C'est cette combinaison de l'expérience terrain de Solucom et de l'appréhension par l'AUSIM des préoccupations et des contraintes des organisations marocaines, enrichie d'échanges fructueux avec plus d'une dizaine de ses membres, qui a permis la réalisation de ce livre blanc, qui se veut un guide pratique pour la mise en conformité.

## La loi 09-08, un enjeu clé ...

Le programme Maroc Numeric 2013 pose une ambition claire : celle d'élever au Maroc au rang mondial qui devrait être le sien, en agissant sur le levier de développement économique et humain que sont les technologies de l'information.

La protection de la vie privée doit être au cœur de ce projet ; Il s'agit d'un

défi que le Royaume entend aujourd'hui relever, en se dotant de la Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à laquelle les organismes marocains doivent à présent se conformer. Fruit d'une réflexion qui fait écho à celles déjà menées en Europe, celle-ci permet au législateur de répondre à cette double préoccupation, du citoyen, et des partenaires internationaux.

Pour les entreprises, outre le respect d'une nouvelle obligation légale, il s'agit dès lors également de maintenir puis faciliter les échanges avec ses partenaires européens et de protéger son image, voire de faire de son souci de la protection de la vie privée un véritable atout concurrentiel. Ainsi, si l'éventail de sanctions prévues s'étend jusqu'à 300 000 Dh d'amende et 2 ans d'emprisonnement, il convient dès à présent de prendre la pleine mesure des enjeux connexes, purement métiers, et qui demain, deviendront prééminents.

### ... pour une mise en œuvre complexe

La loi 09-08 a pour objet l'encadrement des traitements de données à caractère personnel. Si les exigences qu'elle pose pour cela sont relativement claires et dénuées d'ambiguïté, les définitions qu'elle donne de ces traitements et de ces données à caractère personnel sont quant à elles extrêmement larges, et englobent généralement la quasi-totalité du système informatique et des procédures manuelles des organismes.

Du fait de ce périmètre, le réalisme s'impose : seule une démarche pragmatique et structurée, adaptée à chaque organisme, à son organisation et à sa culture, permettra une mise, et surtout un maintien en conformité efficace et à moindres coûts.

### Les cinq piliers de la mise en conformité

Un riche retour d'expérience existe en Europe et le livre blanc permet de mettre en évidence les cinq piliers suivants, sur

lesquels il conviendra de bâtir une telle démarche :

#### 1) Adopter une démarche centrée sur le traitement

La mise en œuvre d'une approche centrée sur la donnée constitue un écueil classique de ce genre de projet : longue et coûteuse, elle ne permet pas d'apporter les mêmes réponses qu'une démarche construite autour de la notion de traitement.



### Association des Utilisateurs des Systèmes d'Information au Maroc

#### 2) Prioriser en fonction du risque juridique

L'exhaustivité immédiate est contre-productive : les entreprises parcourant le plus facilement et le plus rapidement leur chemin vers la conformité sont ainsi celles qui ont su hiérarchiser les traitements et les exigences, et de ce fait initier un véritable cercle vertueux de la conformité.

#### 3) Mobiliser les bons acteurs

Un tel projet nécessite la mobilisation coordonnée d'une multitude d'acteurs, à la fois métiers, SI, juridiques et sécurité. C'est donc bien une véritable gouvernance de la conformité qu'il convient de penser en amont.

#### 4) Traiter la conformité dans sa globalité

Une erreur couramment rencontrée consiste à limiter la mise en conformité aux formalités déclaratives. Bien au contraire, l'essentiel des efforts doit être porté sur les autres exigences de la loi, principalement l'information et le respect des droits des personnes, l'application du principe de proportionnalité et la sécurité des données.

#### 5) Instaurer une véritable culture conformité

Enfin, les efforts doivent être maintenus dans le temps, afin d'éviter la dérive naturelle du niveau de conformité, due aux évolutions des activités, des pratiques ou des systèmes d'information.

#### Quels délais de mise en œuvre ?

Depuis sa promulgation, la loi 09-08 est applicable. Ainsi, tout nouveau traitement doit d'ores et déjà être conforme, les organismes disposant en revanche d'un délai de deux ans pour mettre en conformité l'ensemble des traitements préexistants. Si les experts ne s'accordent pas sur la lecture à avoir de ce délai, tous en fixent l'échéance entre mars et novembre 2012.

#### Saisir l'opportunité de la nouveauté pour mieux affronter les défis de demain

D'ores et déjà, la réflexion est plus qu'amorcée au sein de nombreux organismes.

Sous la pression d'un grand public de plus en plus averti et d'un paysage concurrentiel de plus en plus mature, le niveau d'exigence en matière de conformité ne fera que croître. Par ailleurs, au fur et à mesure que la pédagogie laissera place à la sanction, il est fort à parier que les exigences de la loi iront en se durcissant.

Par conséquent, bien plus que de se mettre en conformité à une nouvelle loi, il s'agit de se familiariser dès aujourd'hui, à son rythme, avec ce qui permettra demain de répondre à des impératifs bien plus grands et bien plus pressants.

Ainsi, l'absence logique d'une doctrine claire sur le sujet ne doit pas être subie, mais au contraire perçue comme une opportunité unique de participer à l'élaboration de cette doctrine. Ce vide toute relatif offre un droit précieux à l'erreur pour les organismes qui, même tâtonnant, auront joué le jeu de la mise en conformité. ■

Abonnez-vous et recevez gratuitement  
votre newsletter et votre magazine .

[www.TechnoMag.ma](http://www.TechnoMag.ma)

Suivez-nous :



Cette rubrique est parrainée par : **Maroc Numeric Cluster**

# La logique Cloud et SaaS pour la PME marocaine

L'évolution rapide d'une technologie peut emmener les utilisateurs et une partie des spécialistes vers une grande confusion entre les besoins des utilisateurs, les opportunités fonctionnelles offertes et les usages qui en découlent. La quantité considérable d'informations relatives au Cloud Computing disponibles actuellement sur le web et les différents supports offline, ne font qu'accroître cette confusion !

Au Maroc comme ailleurs, le Cloud est à la mode, mais derrière une couche marketing épaisse se cache une approche technologique susceptible d'impacter de manière profonde et durable le métier des professionnels de l'informatique et du web. La question paraît complexe tant qu'il existe un large choix de services et de logiques différentes : externalisation complète ou partielle vers « le nuage », mise en œuvre de Cloud privé ou partagé, adaptation d'applications desktop en web applications... Ce « Cloud » est perçu par certains comme une appellation en vogue, de services déjà existant sur le marché.

## Que gagnerait la PME ?

De prime abord, un dirigeant de PME peut ne pas se soucier de la technologie utilisée dans la plateforme d'hébergement de son site web ou le concept ayant servi à créer son logiciel fétiche de gestion, il se préoccupe surtout des fonctionnalités offertes, leur coût et leur disponibilité.

Grâce au Cloud et surtout au SaaS, la PME marocaine gagne en mobilité, en haute disponibilité des informations, mais surtout, en coût d'utilisation très modéré.

Plusieurs solutions sont offertes à la PME marocaine aujourd'hui, nous citerons la mise en place de serveurs Cloud privés, l'hébergement de sites web à haute disponibilité qui commence à apparaître chez les prestataires marocains, mais aussi, des solutions métier touchant le quotidien du manager comme «AutoJahiz» pour les agences de location de voitures, «Ajiel» pour la paie et RH, «BP212» en solutions de gestion ou «Greendizer» pour la gestion de facturation.

## L'hébergement web et le Cloud

L'externalisation des données informatiques (partage de fichiers, sites web, applications métier) vers «le nuage» passe éventuellement par un hébergeur web, le choix d'un prestataire de confiance est influencé en grande partie par la qualité de son infrastructure et de son support client. Outre la haute disponibilité des serveurs web, la technologie Cloud couplée à l'offre abondante d'espaces de stockage permet aux hébergeurs web d'offrir plus d'espace à moindre coût, mais aussi, d'enrichir la palette des services offerts. La mode n'est plus aux serveurs privés virtuels ou autres serveurs dédiés, mais plutôt aux serveurs Cloud que le client peut ajuster à la demande.

Le SaaS comme modèle économique Avec les multitudes solutions web qui voient le jour sous le modèle SaaS, les entreprises marocaines se passeront de l'acquisition ou le développement coûteux d'applications web et desktop, pour passer à des applications web dont les ressources sont partagées, exemple fait par les applications citées plus en avant, qui permettront au manager de la PME d'avoir accès aux fonctions dont il a besoin, quelque soit l'endroit où il se trouve, ou le terminal qu'il utilise, sous réserve de disposer d'une connexion au réseau internet.

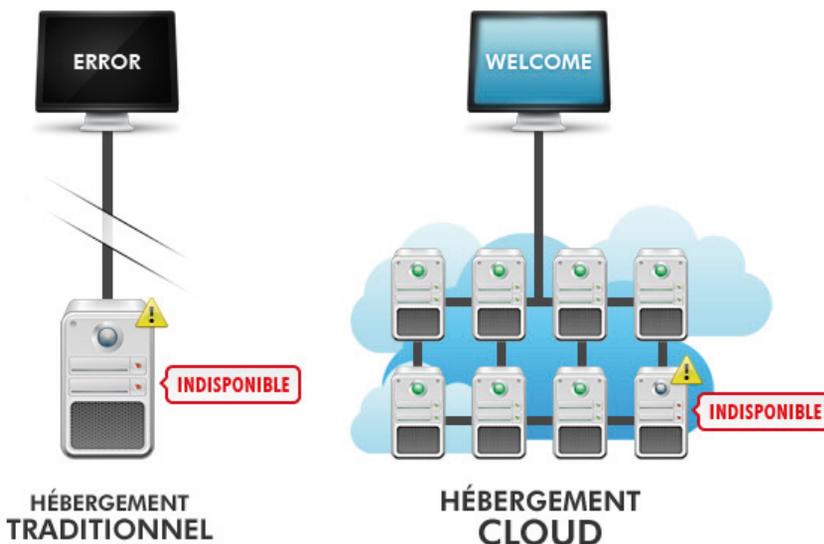
Le SaaS est d'ailleurs plus à prendre comme un modèle économique qui consiste à payer l'utilisation et non le développement du service demandé. Ce modèle d'applications est l'aboutissement même de la technologie Cloud où l'on dépasse la seule vision des solutions techniques, afin d'arriver à une « Logique Cloud » où l'utilisateur fait confiance totale à l'espace virtuel.

## How Cloud Are We?

Malgré le fait que les applications SaaS soient apparues depuis plusieurs années, cette logique Cloud n'est qu'à ses débuts chez la PME marocaine. Cette logique qui rassemble un aspect technique et un autre économique peine encore à gagner la confiance des utilisateurs finaux à cause d'un vecteur essentiel qui est le respect des valeurs éthiques. Le Maroc a répondu à cette crainte avec l'adoption en 2009 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, mais aussi, avec le label eThiq@ qui instaure un climat de confiance vis-à-vis des fournisseurs de services web de manière générale.

Les bases de données clients ou les documents professionnels sont des éléments sensibles chez chaque entreprise; De ce fait, ces informations ne seront pas mises n'importe où ! La confiance constitue le seul moyen de travailler efficacement dans un environnement numérique.

Alors ? Cloud ou pas Cloud ? ■



www.adk-media.com

# “ Le Cloud nous a permis de diversifier notre offre d'hébergement web en diminuant les prix jusqu'à 80% ”



**Driss LEBBAT**  
Directeur Général, ADK Media

• **TM : Selon les prévisions des cabinets d'études internationaux, l'industrie TI mondiale doit enregistrer une croissance soutenue en 2012, tirée par la performance de l'hébergement web et de services Cloud. Quelles innovations majeures pourraient cultiver cette croissance ?**

Tout d'abord, nous devons préciser une chose très importante. Nous avons vécu un vrai phénomène "Cloud" ces derniers mois, alors que les technologies de virtualisation, de stockage et de développement existaient déjà, le Cloud n'est pas une technologie nouvellement créée, mais un environnement qui englobe un ensemble de technologies et d'infrastructures qui, une fois associés, nous font bénéficier d'une haute disponibilité, de l'évolutivité et d'une grande mobilité.

Au niveau professionnel, le passage des ERP, CRM et autres progiciels de gestion vers des versions SaaS ne fera qu'améliorer la logique Cloud dans l'esprit de l'utilisateur final, ce dernier étant déjà familier avec des outils grand public comme DropBox, Evernote, iCloud ou le Google Drive lancé récemment. La bureautique sur le Cloud est aussi un marché voué à un grand avenir, Microsoft

et Google ont déjà annoncé la couleur avec l'Office 365 et Google Apps, il reste aux prestataires tiers de favoriser leur utilisation au sein des entreprises.

Plusieurs études internationales montrent que la virtualisation et le Cloud computing se sont définitivement inscrits dans le paysage informatique professionnel; J'espère qu'au niveau du Maroc, les DSI et autres managers s'adapteront rapidement à cette logique, en adoptant un Cloud privé ou en faisant confiance au Cloud public. Cette technologie offre beaucoup d'avantages concrets, mais il ne faut pas se précipiter à choisir n'importe quelle solution, il faut prendre son temps pour étudier son besoin, choisir le bon partenaire mais surtout, avoir conscience des bonnes pratiques à adopter dans cette ère de Cloudmania.

• **TM : Vous avez récemment annoncé un passage de votre plateforme d'hébergement sur une infrastructure Cloud, qu'est ce cela a changé vis-à-vis à votre service d'hébergement ?**

Nous étions très heureux d'offrir à nos clients au Maroc comme à l'étranger, une nouvelle infrastructure lancée officiellement au mois d'Avril 2012, se basant sur des technologies innovantes que nous avons testées pendant plusieurs mois. Nous avons choisi d'utiliser VMWare comme solution de virtualisation pour nos serveurs et CloudLinux comme système d'exploitation, ces deux partenariats majeurs nous ont permis d'avoir des systèmes stables et hautement performants.

Le Cloud nous a permis de diversifier notre offre tout en diminuant les prix de façon très importante, cela avoisine les 80% de différence par rapport à nos anciens prix. Dans un avenir très proche, les serveurs dédiés et autres serveurs privés virtuels (VPS) céderont définitivement la place aux serveurs Cloud. Ces derniers permettent au client de commander des serveurs paramétrables à la demande, au lieu de choisir parmi des configurations pré-établies.

Dans un système traditionnel, les pannes des serveurs ou les arrêts pour maintenance de sécurité pouvaient causer des coupures aux sites web, ces coupures ne sont plus d'actualité puisque les données informatiques migrent dans le Cloud dès qu'un dispositif matériel est signalé en défaillance, permettant ainsi une haute disponibilité de tous nos packs d'hébergement. La sécurité également gagne dans cette nouvelle infrastructure, puisque les ressources des packs d'hébergement sont virtuellement séparées, le risque d'inter-hacking est quasiment inexistant ; Aussi, la gestion améliorée des ressources systèmes permettent une meilleure expérience utilisateur. Dans un environnement mutualisé par exemple, un site web qui consomme les ressources matérielles de façon excessive n'affecte plus la bonne marche des autres sites hébergés sur la même infrastructure.

• **TM : Êtes vous confiants dans l'avenir de l'hébergement web et des solutions Cloud au Maroc ?**

Avec tous ces changements et la diminution des coûts pour les utilisateurs finaux, nous ne pouvons qu'être plus compétitifs au niveau mondial. Chez ADK Media, nous prévoyons l'ajout de plusieurs produits à notre panel, mais surtout, augmenter le volume d'exportation de nos services vers les pays arabes et africains, grâce à un large réseau de revendeurs.

## biographie

A 34 ans, Driss Lebbat tire derrière lui une expérience de 12 ans dans le domaine du web, un véritable web entrepreneur ayant lancé plusieurs projets avant de cofonder la société ADK Media en 2006, l'une des toutes premières entreprises marocaines à offrir des services d'hébergement cloud et de développement web au Maroc.

Driss Lebbat est aussi calligraphe, blogueur et membre très actif de la communauté web marocaine. ■

## Neuf moyens pour protéger les identités des utilisateurs des réseaux sociaux

Les sites de réseaux sociaux gagnant en popularité, le risque de voir son identité volée s'avère plus élevé que jamais. Voici les étapes essentielles que les consommateurs et les entreprises doivent suivre afin de protéger leur identité et celle de leurs utilisateurs sur les sites de réseaux sociaux et autres.

### Nous préconisons aux consommateurs de:

1. Créer des mots de passe uniques et complexes. Il est recommandé de créer des mots de passe composés de séries de chiffres, lettres et symboles quelconques et de ne jamais utiliser le même mot de passe sur plusieurs sites.

2. Utiliser une application mobile de coffre-fort de mots de passe pour faciliter la recommandation n°1. Une application mobile de coffre-fort de mots de passe vous permet de générer automatiquement des mots de passe uniques à vingt ou trente caractères, comprenant des séries de chiffres, lettres et symboles impossibles à retenir. Il est possible de sécuriser le coffre-fort à l'aide d'un code PIN de téléphone mobile, créant ainsi instantanément deux niveaux de protection.

3. Modifier fréquemment ses mots de passe. Même si votre mot de passe bien pensé est divulgué d'une quelconque manière (par phishing sur un site de réseaux sociaux, par exemple), cela vous garantit que personne ne pourra l'utiliser longtemps.

4. Vérifier souvent ses comptes. Connectez-vous régulièrement à tous vos sites de réseaux sociaux et assurez-vous qu'aucun envoi d'e-mail, mise à jour de statut ou autre activité inopinée n'apparaît.

5. Utiliser des gestionnaires d'identité. Des services suivant votre identité, tels que Reputation.com et LifeLock.com, peuvent vous prévenir en cas de vol d'identité. Cette étape s'avère essentielle pour réduire les impacts éventuels.



6. Ne jamais cliquer sur les liens contenus dans des e-mails ou messages. Si vous devez cliquer sur ce lien, ne saisissez jamais votre identifiant ou mot de passe une fois sur le site, même s'il vous paraît un site familier de réseau social.

### Nous préconisons aux entreprises de:

1. Offrir à leurs utilisateurs une forme de double authentification ou une authentification à deux facteurs. Les entreprises proposant d'envoyer un SMS sur le téléphone mobile d'un utilisateur inscrit dans le cadre du processus de connexion, renforcent considérablement la sécurité de l'utilisateur.

2. Protéger les identifiants de leurs employés. Lorsqu'ils se connectent à un réseau privé virtuel, les employés utilisent souvent les mots de passe de leurs réseaux sociaux favoris. S'ils sont interceptés et qu'un hacker associe l'employé à l'employeur, il peut accéder à l'ensemble du réseau de l'entreprise.

3. Promouvoir une solution de connexion unique de Single Sign On. De nombreuses solutions de connexion unique peuvent stocker les mots de passe sous forme cryptée et déconseiller automatiquement aux employés d'utiliser leur mot de passe d'entreprise sur les sites de réseaux sociaux et autres. Tirez pleinement parti de ces solutions.

Les vols d'identité sont une réalité de notre société moderne. Cependant, si les consommateurs et les entreprises suivent les recommandations ci-dessus, les utilisateurs pourront jouir des avantages des réseaux sociaux sans mettre en péril leur identité numérique. ■

## Lancer un sondage sur Facebook



Si l'envie vous prend de lancer un sondage sur le réseau communautaire Facebook, pour avoir un avis sur un futur achat ou tâter le terrain concernant une soirée à venir

par exemple, sachez qu'il existe un outil intégré prévu à cet effet. Voici comment y accéder et s'en servir.

Une fois arrivé sur la page d'accueil, il

suffit de cliquer sur le bouton "Question", qui se trouve juste derrière des boutons nommés "Statut" et "Photo / vidéo". Il ne restera ensuite qu'à saisir la question, indiquer les réponses (qui pourront d'ailleurs être complétées ou non par les participants au sondage), choisir le groupe de personnes à sonder et publier le tout sur votre mur.

Pas forcément indispensable, l'outil est là. Il serait donc assez dommage de s'en priver. ■

# Hmizate.ma

## Hi-Tech



**Site E-Commerce de l'année**

## Et oui, un site populaire ne veut pas, toujours, dire un site sécurisé



**S**SL Pulse met en lumière l'implémentation du protocole de sécurité SSL (ou TLS) pour près de 200 000 sites parmi les plus populaires au monde. Seulement 10% des sites sont considérés comme véritablement sécurisés.

Le projet SSL Pulse est présenté comme un tableau de bord dont l'objectif est de rendre compte de l'implémentation de SSL (Secure Socket Layer) sur le Web. L'outil sert surtout à mettre en lumière le fait que cette implémentation laisse souvent à désirer.

Également connu sous le nom de TLS (Transport Layer Security), SSL est un protocole de sécurité qui chiffre les données sensibles lors de transactions en ligne. Devenu pierre angulaire de la sécurité sur Internet, la manière de son déploiement peut néanmoins compromettre cette sécurité.

Avec pour socle SSL Labs de Qualys, SSL Pulse vérifie par exemple la longueur des clés, les versions des protocoles pris en charge par des sites

en HTTPS. Il peut s'agir de SSL 3.0, TLS 1.0 ou mieux TLS 1.1 voire 1.2 si possible. SSL 2.0 est par contre à proscrire, cette version n'étant plus sûre.

SSL Pulse s'intéresse à près de 200000 sites SSL considérés comme les plus populaires au monde en fonction du classement Alexa. Près de 50 % des sites ont obtenu la note de A, ce qui signifie que les autres sites doivent améliorer leur configuration de SSL.

### SSL Security Summary



Mais même avec une note de A, et donc une bonne configuration de SSL, des faiblesses demeurent au niveau du

support de la renégociation SSL ou d'une vulnérabilité à une attaque BEAST. Au bout du compte, la première analyse de SSL Pulse estime que seulement 10 % des sites sont véritablement sécurisés. Une mise à jour mensuelle permettra de suivre les progrès réalisés par les sites.

SSL Pulse est une initiative du Trustworthy Internet Movement (TIM) mis en place par des experts en sécurité et entrepreneurs irrités par la lenteur des améliorations pour la sécurité en ligne. L'organisme à but non lucratif a été fondé par le président et PDG de Qualys.

Le premier projet du TIM est la gouvernance SSL et des propositions en vue d'une meilleure protection sur Internet. Un groupe de travail est constitué d'experts venus de PayPal, Google, Qualys, Whisper Systems (réemment acquis par Twitter), GMO GlobalSign (fournisseur de certificats SSL). L'un des créateurs du protocole SSL, Taher Elgamal, est également impliqué. ■

# VERIFIEZ VOS ACHATS POUR EVITER LA CONTREFAÇON



**Assurez-vous  
que c'est de  
l'original HP !**

**S**oyez prudents lors de vos achats afin de vous protéger des contrefaçons. N'effectuez vos achats qu'auprès des revendeurs agréés HP, évitez les offres suspectes sur Internet, et si une bonne affaire semble être trop bonne pour être vraie, c'est probablement le cas !

Les contrefacteurs ne souhaitent que vous faire croire que leurs fausses marchandises sont aussi bonnes que les produits de marque originaux mais ce n'est pas le cas. Lors de l'achat d'un logiciel, DVD -ou tout autre produit- il est important que vous vous assuriez de recevoir la qualité original pour laquelle vous payez.

Les contrefaçons ne répondent pas aux spécifications rigoureuses des produits authentiques ; ils ne fonctionnent pas aussi bien. Ce qui peut nuire à l'acheteur et détruire les ordinateurs et les périphériques et annuler la garantie du produit. Les contrefaçons sont illégales. Elles nuisent aux marchands honnêtes et suppriment de nombreux emplois légitimes.

Si on considère les fournitures d'impression comme exemple. Seul l'encre et le toner authentiques sont soutenus par des décennies d'investissement et d'essais pour produire la plus constante et fiable des qualités d'impression. Les photos imprimées avec les encres de la marque HP et sur le papier HP, par exemple, dure plus de 60 ans que celles imprimées avec l'encre non-HP<sup>1</sup>.



## Comment vérifier et déceler une contrefaçon

➤ **Lors de l'achat**, cherchez le label de sécurité HP. Inclinez le devant de la boîte vers l'arrière pour vous assurer de voir le mouvement de 'OK' et '✓' dans les directions opposées; inclinez également la boîte de droite à gauche pour voir le mouvement des symboles dans la même direction. La dernière génération de ces labels dispose également des codes QR que vous pouvez capturer à l'aide d'une application sur votre Smartphone qui valident l'authenticité du produit. Vous pouvez aussi accéder au site Web HP mentionné sur les nouvelles étiquettes de sécurité [www.hp.com/go/ok](http://www.hp.com/go/ok), puis saisissez le numéro de série de l'étiquette pour la valider.



➤ **Après l'achat**. Le logiciel de l'authentification indique si la cartouche insérée est d'Origine HP et vous avertit si elle ne l'est pas. Le téléchargement et l'installation du logiciel est facile; il suffit d'aller sur le site [www.hp.com/go/tonercheck](http://www.hp.com/go/tonercheck) (le logiciel de vérification de la cartouche d'encre est préinstallé sur l'imprimante).

un nouveau mode de vie

# MAZONE

## Site de vente privée

Pourquoi se priver quand on peut faire les soldes toute l'année ?



[www.mazone.ma](http://www.mazone.ma)  
Le luxe à portée de main

