Septembre 2015 | n°138

www.linformaticien.com

L'INFORMATICIEN

Maîtriser WINDOWS 10
Ce qu'il faut absolument savoir

Ouvrage offert avec votre abonnement !

6 MENACES À ÉRADIQUER

- VOL DE DONNÉES
- DDOS
- INGÉNIERIE SOCIALE
- PHISHING
- MAN IN THE MIDDLE
- DÉFACEMENT

SILICON VALLEY
Les dernières tendances ?
SDN, Flash et… Open Source

POWER BI 2.0 : une Self-BI immédiate et accessible

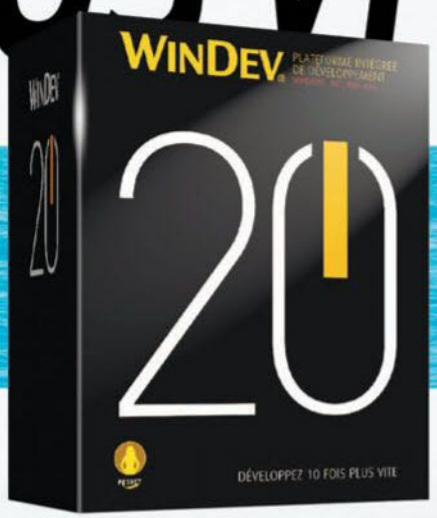
FRAMEWORK QT 5.5 : quoi de neuf sous le soleil ?

M 08064 - 138 - F: 5,40 € - RD
PCpresse
France : 5,40 € / Bel. : 6,00 € / CH : 10,50 FS / Canada : 10,50 $CAN

WINDEV
DÉVELOPPEZ
10 FOIS
PLUS VITE

Elu
«Langage
le plus productif
du marché»

140 pages de témoignages de sociétés
prestigieuses sur simple demande
(également en PDF sur pcsoft.fr)



Développez une seule fois,
et recompilez pour chaque cible.
Vos applications sont natives.

VERSION
EXPRESS
GRATUITE
Téléchargez-la !

Windows
Linux
Mac
Internet
Cloud
WinPhone
Android
iOS
...

Tél province: **04.67.032.032**
Tél Paris: **01.48.01.48.88**

Fournisseur Officiel de la Préparation Olympique

www.pcsoft.fr
120 témoignages sur le site

RENTRÉE EN ACCÉLÉRÉ

L'un des freins au développement plus rapide de la voiture électrique est la longueur de chargement des batteries. Ainsi que le peu d'équipements disponibles dans le véhicule. Il en va de même, bien que dans des proportions moindres, pour tous nos appareils mobiles, smartphones et autres tablettes. Une start-up israélienne propose de régler ce problème de manière définitive. En effet, Storedot affirme que ses technologies permettent de recharger intégralement un smartphone en moins d'une minute et un véhicule électrique en moins de cinq minutes, soit le temps moyen de passage à la station pour faire un plein de carburant traditionnel. Les produits devraient être disponibles dès l'année prochaine, du moins le chargeur pour smartphone. Cet exemple, parmi des dizaines d'autres, montre que les progrès technologiques sont loin de s'essouffler dans de multiples domaines et venant de tous les horizons, à la notable et malheureuse exception de l'Europe. La robotique est un autre domaine qui progresse à une vitesse proprement ahurissante dans de nombreuses directions et pour des usages très divers. Pour servir toutes ces avancées, il faudra bien évidemment compter sur l'augmentation de la puissance informatique, le big data et l'intelligence artificielle. Tous ces domaines voient également des avancées quotidiennes. Dans le domaine de l'IA, et comme nous l'indiquions dans notre dossier paru au mois de mai dernier, les grands acteurs de l'informatique et de l'Internet sont en pointe sur le sujet. Très prochainement, IBM va proposer un processeur baptisé TrueNorth composé de 48 millions de cellules nerveuses artificielles capable d'avoir une puissance de calcul équivalente à celle du cerveau d'une souris. De telles puces pourraient équiper nos smartphones d'ici à quelques années et les logiciels capables d'en tirer parti existent déjà chez Facebook, Google ou Microsoft pour ne citer que quelques fers de lance de l'IA.

MAÎTRES DU JEU

Voici de nouveaux exemples de l'accélération des progrès technologiques tels que nous en faisons état à intervalles réguliers. Répétons-le : tous ceux qui croient à un ralentissement, voulu ou non, en particulier pour les questions éthiques qui ne manqueront pas de survenir, se trompent lourdement. Les organisations et les dirigeants politiques sont complètement dépassés ! En témoigne – là-aussi régulièrement – des décisions législatives inopérantes, inapplicables, voire imbéciles, où qu'ils se trouvent sur l'échiquier. Les Gafa (Google, Apple, Facebook, Amazon), les Natu (Netflix, AirBnB, Tesla, Uber) et les Unicorns, sociétés privées valorisées plus de 1 milliard de dollars, sont les maîtres du jeu. Qu'on le veuille ou non.

Stéphane Larcher, directeur de la rédaction :

Vous croyez **encore que le** *Cloud Computing* **est cher ?**

Avec ArubaCloud,

Vous avez accès à une large gamme de solutions de Cloud Computing, avec choix du pays du datacenter utilisé, solution packagée ou flexible avec facturation adaptée..
Vous pouvez dès maintenant créer votre serveur Cloud SMART à partir de 1€ht / mois.

*Prix Hors Taxe, vérifiez la liste des prix pour plus d'informations

**MON PAYS, MON CLOUD.

Hyperviseur vmware

Contrôle des coûts

6 datacenters en Europe

APIs et connecteurs

Linux & Windows

1 Quitte à choisir une infrastructure IaaS, autant prendre la plus performante!
Aruba Cloud est de nouveau **N°1 du classement des Cloud**
JDN / CloudScreener / Cedexis (Janvier 2015)

Contactez-nous! 0810 710 300 www.arubacloud.fr

aruba CLOUD

Cloud Public | Cloud Privé | Cloud Hybride | Cloud Storage | Infogérance

MY COUNTRY. MY CLOUD.**

sommaire

Maîtriser WINDOWS 10 : ce qu'il faut absolument savoir p. 78

SÉCURITÉ : 6 MENACES À ÉRADIQUER p. 38

Power BI 2.0 : une Self-BI immédiate et accessible p. 61

Tendances Silicon Valley : SDN, Flash et Open Source p. 29

«Les systèmes de demain doivent être beaucoup plus prédictifs»

Alex Dayon, Président Produits, Salesforce.com p. 20

LE CLOUD GAULOIS, UNE RÉALITÉ ! VENEZ TESTER SA PUISSANCE

EXPRESS HOSTING

Cloud Public
Serveur Virtuel
Serveur Dédié
Nom de domaine
Hébergement Web

sales@ikoula.com
01 84 01 02 66
express.ikoula.com

ENTERPRISE SERVICES

Cloud Privé
Infogérance
PRA/PCA
Haute disponibilité
Datacenter

sales-ies@ikoula.com
01 78 76 35 58
ies.ikoula.com

EX10

Cloud Hybride
Exchange
Lync
Sharepoint
Plateforme Collaborative

sales@ex10.biz
01 84 01 02 53
www.ex10.biz

l'œil de Cointe

INFOS BOURSE

PayPal désormais coté au Nasdaq

Valeurs US

Valeurs	Cours	Tendances	Capitalisation
Apple	115,96 $	↘	661,287
Microsoft	47 $	↗	375,9
Google	657,12 $	↗	331,221
Facebook	94,42 $	↗	266,032
Amazon	531,52 $	↗	248,597
IBM	155,74 $	↘	152,552
Intel	29 $	↘	137,94
Cisco	29 $	↗	147,64
HP	28,49 $	↘	144,89
Twitter	29,07 $	↘	19,66

Valeurs FR SSII & éditeurs

Valeurs	Cours	Tendances	Capitalisation
Dassault Systèmes	67,09 €	↗	17,1
Capgemini	85,13 €	↗	14,65
Gemalto	76,54 €	↘	6,8
Atos	68,62 €	↗	7,06
Ingenico	124,80 €	↗	7,61
Ubisoft	17,55 €	↗	1,95
Altran	10,19 €	↗	1,78
Sopra Steria	99,31 €	↗	2,026
Econocom	8,45 €	↗	0,95
Gameloft	3,90 €	↘	0,33

Depuis le 21 juillet, PayPal est désormais indépendant d'eBay : le service de paiement en ligne a fait son entrée sur les marchés financiers et l'action s'est rapidement envolée, prenant plus de 6 % après les premiers échanges, à 40,70 dollars. Elle est depuis retombée à 38,14 dollars – le 17 août. Parallèlement, le groupe a cédé Magento, la solution e-commerce open source, rachetée 2,4 milliards de dollars en 2011.

Valeurs FR Réseau & Mobilité

Valeurs	Cours	Tendances	Capitalisation
Orange	14,62 €	↗	38,68
SFR-Numericable	48,08 €	↗	21,07
Iliad	217 €	↗	12,65
Thales	61,75 €	↗	12,92
Alcatel-Lucent	3,17 €	↘	8,96

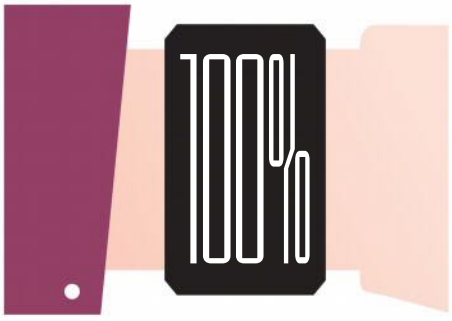
Valeurs EU

Valeurs	Cours	Tendances	Capitalisation
SAP	62,80 €	↘	77,15
Ericsson	9,36 €	↘	30,81
Nokia	6,61 €	↗	23,21
Software AG	26,43 €	↗	2,08
Sage	7,28 €	↘	7,8

Les capitalisations boursières sont exprimées en milliards. Les variations (à la hausse, à la baisse) des cours boursiers le sont d'un mois sur l'autre. Cours relevés le 17 août 2015 et comparés à ceux du 19 juin 2015.

LA TENDANCE SÉCURITÉ

Les smartwatches sont vulnérables !



Carton plein ! Aucune montre connectée n'échappe à des vulnérabilités. Vous me direz, pour n'importe quel spécialiste de la sécurité, il n'y a rien de bien étonnant. Surtout que nous sommes en l'An zéro des « smartwatches ». Alors, à quoi bon s'embêter à poser des verrous partout là où il en faudrait ? 100 % des montres vulnérables, c'est donc ce qui ressort d'une étude de HP Fortify. Et même si les noms des modèles ne sont pas précisés, l'Apple Watch est dans la liste. Le pire, c'est que tout y passe : DNS en standalone, sécurité des interfaces cloud et mobiles, transmission des données… Si bien que 40 % des modèles étudiés sont vulnérables aux attaques POODLE. « *Connectez-vous* », qu'ils disaient… !

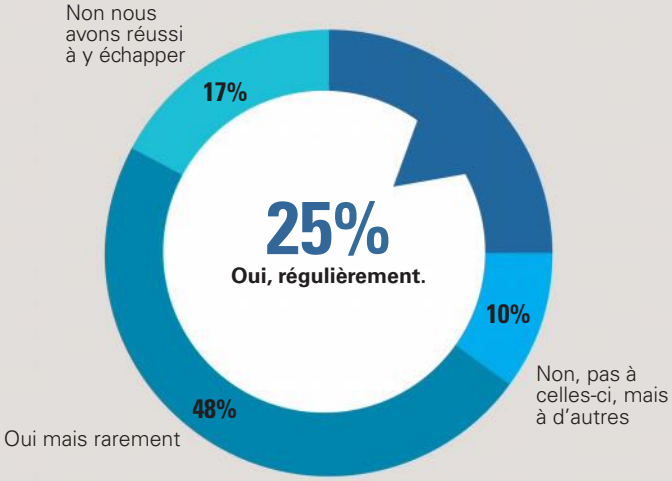
ENQUÊTE EXPRESS

Vol de données, phishing, défacement, Man in The Middle, déni de service...

Face aux menaces, comment réagir ?

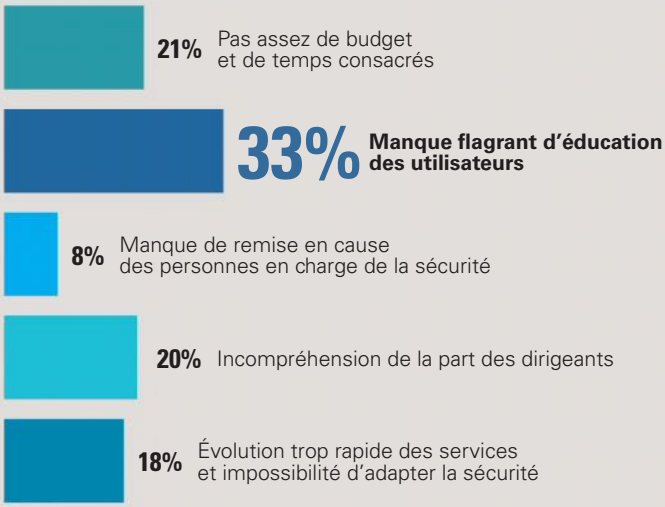
Enquête réalisée en juillet-août 2015 auprès des visiteurs du site linformaticien.com

1 Avez-vous professionnellement été déjà confronté à ces différents types de menaces ? (une seule réponse)



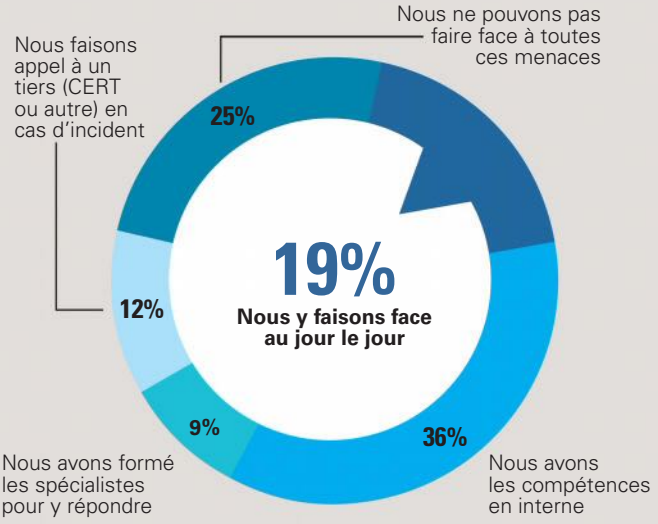
Un quart des entreprises sont régulièrement sujettes à ces attaques.

2 Selon vous, d'où viennent les problèmes de sécurité en entreprise ? (plusieurs réponses)



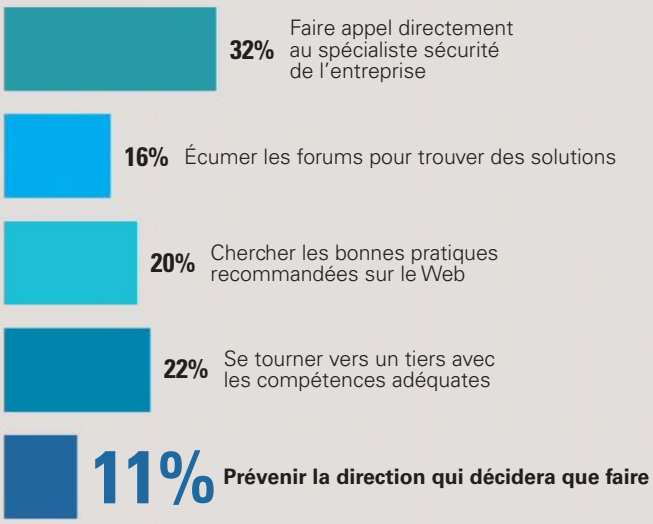
Le manque d'éducation reste le facteur de diffusion prédominant.

3 Au sein de votre entreprise, comment appréhendez-vous ces menaces ? (une seule réponse)



Se protéger avec les moyens du bord est encore courant.

4 Quels sont vos réflexes face à ce genre de menaces ? (plusieurs réponses)



La direction encore peu concernée par la sécurité informatique.

Emploi IT

Pôle Emploi confirme l'embellie dans l'IT

Le chômage IT encore en baisse…

Le nombre de chômeurs dans le domaine des systèmes d'information a baissé récemment, malgré une très faible hausse en mai dernier. Mais en juin, le nombre est passé sous la barre des 36 000, à 35 800 chômeurs de catégorie A, selon les derniers chiffres communiqués par Pôle Emploi.
En revanche, dans les catégories ABC cumulées, 45 100 demandeurs étaient encore inscrits en juin 2015, soit 100 de moins que le mois précédent. Les métiers de l'IT confirment une nouvelle fois leur bonne forme vis-à-vis du monde du travail en France en général. Ce n'est d'ailleurs pas dû au hasard puisqu'on a enregistré une hausse de 21 % des offres (17 693) de juin 2014 à juin 2015.

…mais pas d'un an sur l'autre

Les chiffres de l'emploi dans l'IT (ci-dessus) peuvent laisser rêveur, mais pas tout à fait si on les regarde de plus près. En effet, entre 2014 et 2014, on enregistre une hausse des chômeurs de 7 % sur le front du chômage IT (chômeurs de catégorie A) et de +10 % sur les demandeurs des catégories ABC.
Selon les derniers chiffres de l'Apec, le volume d'offres d'emploi dans l'informatique atteint un total de 180 687 propositions cumulées sur un an, soit une progression de +10 %. Dans le détail, les métiers du Web sont ceux qui connaissent la plus forte de demande (+26 %) suivis de l'informatique industrielle (+21 %) et de la maîtrise d'ouvrage ainsi que des directions informatiques (+16 % chacune).

Pôle Emploi roule avec Simplon

C'est une association un peu inédite qui a vu le jour dans l'Indre : Pôle Emploi, l'association Entente des générations pour l'emploi et l'entreprise (Egee) et Simplon.co ; ce dernier propose des *« formations intensives de six mois pour apprendre à créer des sites web, des applications web/mobile, et en faire son métier »*. Vingt demandeurs d'emploi vont donc être formés au développement en utilisant la plateforme de Simplon, le tout financé à hauteur de 11 000 euros par des partenaires.
Un site web a même été monté pour promouvoir l'opération : www.les-codeurs-indriens.fr

Simplonline est un « FOAD », un outil de Formation à Distance en ligne.

Performances du Cloud

SFR tient la corde avec son CDN

Depuis plusieurs mois consécutifs, SFR obtient les meilleurs résultats en termes de temps de réponse et de taux de disponibilité avec son CDN, selon Cedexis.

Cloud — Temps de réponse (en millisecondes)

1er	Ecritel E2C - Paris	42
2e	Mediactive Network	42
3e	Gandi - FR	42
4e	VeePee IP Cloud - Paris	42
5e	SFR Cloud - Courbevoie	42
6e	Cloudwatt	43
7e	Numergy - Paris	43

CDN — Temps de réponse (en millisecondes)

1er	SFR CDN	40
2e	Tata Communications	41
3e	Akamai Object Delivery	41
4e	CDNetworks	42
5e	Mediactive Network	42
6e	Azure CDN	42
7e	Edgecast Small	43

Cloud — Disponibilité (en %)

1er	SFR Cloud - Courbevoie	99,402
2e	Ikoula France	99,397
3e	Aruba Cloud - FR	99,395
4e	VeePee IP Cloud - Paris	99,394
5e	Softlayer - Paris	99,392
6e	Mediactive Network	99,391
7e	Outscale - EU	99,391

CDN — Disponibilité (en %)

1er	Tata Communications	99,371
2e	CacheFly	99,353
3e	Mediactive Network	99,347
4e	Hibernia	99,335
5e	Level3	99,298
6e	Azure CDN	99,283
7e	Cloudfront	99,279

Classement établi en partenariat avec cedexis www.cedexis.com/fr Valeurs moyennes sur juillet 2015.

Parce que vous avez demandé une vision globale.

Présentation du DCIM avec une visibilité du bâtiment au serveur : la suite logicielle StruxureWare for Data Centres.

La visibilité complète dont vous avez besoin

Une vision précise de l'infrastructure physique de votre datacenter depuis le bâtiment jusqu'aux serveurs (et inversement) est impérative pour maintenir l'équilibre entre disponibilité et efficacité. Aujourd'hui, vous devez vous adapter rapidement aux exigences du marché sans mettre en péril la disponibilité ou l'efficacité du système. Une visibilité end-to-end garantit la disponibilité de votre système tout en vous permettant de gagner en efficacité énergétique et opérationnelle.

Trouver le juste milieu

Le logiciel Schneider Electric StruxureWare™ for Data Centers fournit cette visibilité totale en connectant l'informatique aux services généraux. En réalité, notre logiciel avancé de gestion de l'infrastructure du datacenter (DCIM) représente graphiquement votre équipement informatique au sein de l'infrastructure physique du datacenter (du rack à la rangée, puis au bâtiment), si bien que vous pouvez surveiller et protéger la disponibilité du système, et simuler et analyser l'effet des déplacements, ajouts et modifications par rapport à la capacité des ressources et à l'utilisation énergétique. Résultat : Les services généraux et l'informatique peuvent facilement collaborer pour une adaptation permanente du datacenter aux exigences du marché, tout en maintenant l'équilibre entre disponibilité et efficacité énergétique.

Business-wise, Future-driven.™

Maximiser l'efficacité

Améliorer l'efficacité énergétique en identifiant les gaspillages énergétiques du datacenter et en les éliminant.

Optimiser la disponibilité

Atteindre une meilleure disponibilité avec une visibilité complète de l'infrastructure physique de votre datacenter.

StruxureWare

Visibilité end-to-end de votre datacenter

- Visualiser les scénarios de modification/capacité
- Afficher l'efficacité énergétique et l'efficacité de l'infrastructure de votre datacenter (PUE/DCiE) actuelles et historiques
- Maintenir une disponibilité optimale à tout moment
- Afficher et gérer votre consommation énergétique
- Gérer l'espace et les cages des salles accueillant plusieurs clients
- Services de cycle de vie du datacenter renforcés : depuis la planification jusqu'à la maintenance

APC by Schneider Electric

Les produits, solutions et services d'APC™ by Schneider Electric font partie intégrante du portefeuille informatique de Schneider Electric.

Téléchargez le livre blanc !

Visitez le site www.SEreply.com Code clé 79731V

Schneider Electric™

Réseaux sociaux

Internet 100 Mbit/s : cherchez le bonheur !

L'INFORMATICIEN www.linformaticien.com

#HautDébit

***L'Informaticien* a réalisé son palmarès des communes françaises les mieux desservies en haut et très haut débits, en se basant sur les dernières statistiques de la mission Très Haut Débit. Seules 25 communes offrent du THD aussi bien en DSL que via le câble ou la fibre optique FttH.**

Le palmarès !

Nous avons établi deux palmarès, dont un basé sur le taux d'éligibilité à la valeur reine : le FttH à 100 Mbps. Surprise : des villages de Meurthe-et-Moselle, de l'Ain et du Nord figurent en tête du palmarès !

Département	Commune	Part des locaux éligibles Fibre FttH 100 Mbit/s et +
Meurthe-et-moselle	Saulxures-lès-Nancy	98,6%
Ain	Chaneins	97,4%
Ain	Pizay	97,2%
Ain	Sainte-Julie	97,1%
Meurthe-et-moselle	Laneuveville-devant-Nancy	96,7%
Ain	Thil	96,5%
Oise	Heilles	96,3%
Ain	Curtafond	95,4%
Ain	Genouilleux	95,4%
Ain	Farges	95,2%

L'1FO

Vos commentaires sur notre site *Rubrique Débats*

Cette petite enquête a fait réagir, notamment quant à la méthode de mesure et de collecte des données. Mais aussi sur l'installation de la fibre sur tout le territoire.

« La solution de Fibrage par quartier est la meilleure solution et si une entreprise veut se raccorder au NRA, eh bien, elle tire à ses frais la fibre… et basta. »
XP25

Un point de vue vite démonté car :

« Se raccorder au NRA, ça n'a pas de sens puisqu'il faut après se connecter à Internet, c'est-à-dire trouver un loueur de trafic qui va te rapporter à un nœud de peering. »
JD3550

Et un autre lecteur d'ajouter qu'un NRA...

« ... cela ne rapporte absolument rien à la collectivité, au contraire »
Margarita

Pour contribuer à ces discussions – et à bien d'autres –, visitez la rubrique DEBATS du site linformaticien.com

Sur Facebook *Page à liker : l1formaticien*

L'actualité a tourné sur les réseaux sociaux et sur Facebook : une nouvelle preuve que la connexion internet demeure une préoccupation quotidienne des Français.

TOSHIBA

Leading Innovation

La passion de la précision

Fiabilité à long terme et dans les moindres détails.

X300/P300
High-Performance Hard Drives

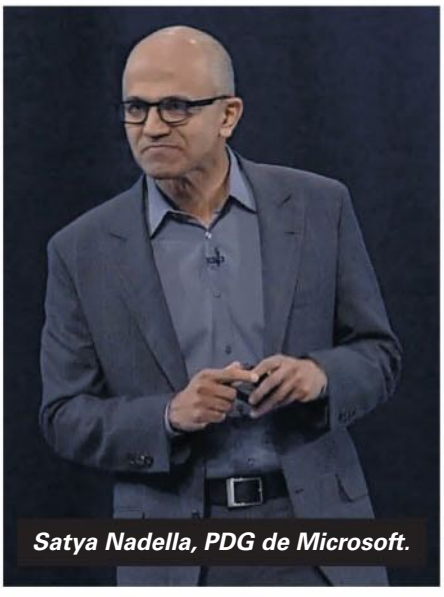
Pour plus d'informations, visitez le site toshiba.fr/internal-hdd

Windows 10, Cortana, Hololens...

Microsoft affiche ses ambitions

Après la litanie des mauvaises nouvelles sur les résultats et la dépréciation des actifs rachetés à Nokia, l'ambiance aura été plutôt sereine à la conférence WPC 2015. Plus de 12 000 partenaires de Microsoft étaient à Orlando, en Floride, où les ambitions réaffichées et les nouveaux produits ont pu alimenter cette « zen attitude » : en exergue, une session très réussie de Satya Nadella.

Pour beaucoup, Microsoft semble naviguer à vue et suivre les tendances du moment sans véritable ligne directrice sur le long terme. La dernière intervention de Satya Nadella devant des milliers de représentants de l'écosystème de l'éditeur devrait mettre un point final à cette vision faussée de la stratégie de Microsoft. L'ambition est de *« transformer et de renforcer les personnes et les organisations pour faire mieux »*. Cette vision se traduit par trois axes fondamentaux : réinventer la productivité personnelle et les process métier en s'appuyant sur le cœur historique de l'offre de Microsoft sur la création, la communication et la collaboration et les lier ensemble pour former de nouveaux ensembles de services pour l'entreprise. Mais Microsoft veut aller encore plus loin en éliminant les limites actuelles du travail de chacun pour une approche concentrée sur le fait de savoir comment les personnes travaillent.



Satya Nadella, PDG de Microsoft.

Aujourd'hui le monde est « multifenêtre » et basé sur des silos d'applications et des silos de données avec lesquels il est souvent difficile de trouver de véritables enseignements pour prendre de bonnes décisions. La démocratisation de ces nouveaux services « sans frontières » utilise pleinement les possibilités du Cloud sur lequel clients et partenaires de Microsoft semblent s'accorder selon les chiffres fournis lors d'une interview de Jérôme Tredan, en charge de l'animation des partenaires vers les petites et moyennes entreprises. Globalement, 42 % des revenus de Microsoft proviennent du Cloud. L'année prochaine, ce sont 50 % qui devraient découler de ce modèle de commercialisation. Si la France est encore un peu derrière sur cette tendance, le changement s'accélère et la division de Jérôme Tredan connaît 15 % de croissance sur les derniers mois avec une forte demande des PME. Ce modèle ne peut cependant se concevoir que si la confiance et la sécurité sont là et Microsoft indique faire un effort particulier dans le domaine.

La montée en puissance de Cortana et Hololens

Les dernières annonces vont dans le sens de Satya Nadella avec des démonstrations assez spectaculaires autour de l'assistant vocal Cortana et du casque de réalité augmentée Hololens qui montent en puissance dans l'ensemble de l'offre Microsoft.

Cortana joue d'ailleurs plusieurs rôles. Tout d'abord il devient une sorte de point d'entrée, vocal ou non, pour l'ensemble des produits de Microsoft, que ce soit dans Windows 10 ou les autres logiciels de productivité de

Une vue d'une moto conçue sur Autodesk avec Hololens.

La même en taille réelle avec la réalité augmentée de Hololens.

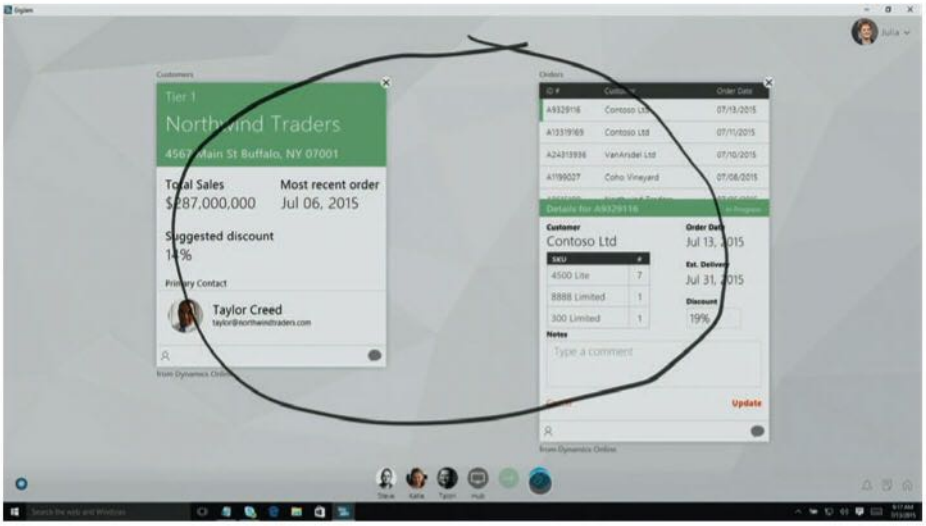
l'éditeur en s'appuyant sur les éléments sémantiques de Cortana. Via Power BI, Microsoft étend les possibilités de Cortana avec une suite analytique qui sera disponible dans les semaines à venir. Plusieurs scénarios pré-établis seront disponibles à partir d'une offre en ligne.
Autre innovation vers les entreprises, le projet Gigjam change véritablement la manière de concevoir le process en entreprise avec la possibilité de lier entre elles des applications et des données pour autoriser un travail en tâches et non plus application par application.
Spectaculaire était la démonstration d'Hololens et son intégration avec les outils d'Autodesk sur une modélisation de moto et les changements en temps réel rendus possibles par la technologie de réalité augmentée.
Les partenaires présents ont dans l'ensemble plutôt bien accueilli les annonces et la stratégie énoncée, même si certains ont exprimé des réserves sur ce qu'il y a véritablement derrière ces nouvelles avancées. Ils sont d'ailleurs généralement satisfaits des partenariats avec Microsoft et du volume d'affaires sur les produits de l'éditeur de Redmond. Les premières interrogations il y a quelques années autour de la transformation vers le Cloud semblent belles et bien oubliées. Comme le résume certains

medias américains commentant les annonces depuis le début de l'année, « Microsoft is back » !

Exploiter la puissance de Power BI

Avec 92 % de ses revenus provenant des ventes indirectes, Microsoft s'appuie sur des partenaires dans tous les domaines de l'informatique, des applicatifs à l'infrastructure en passant par le conseil ou l'intégration. Lors de la manifestation nous avons rencontré deux acteurs intéressants mais aux profils très différents : Novulys et Alterway.

Novulys, créé il y a 4 ans, proposait à ses clients des solutions clés en mains dans les secteurs de la santé et du commerce de détail sur des Clouds privés. Avec la montée en puissance des outils de Clouds publics et d'applications sous forme de services chez Microsoft, Novulys s'est porté sur les outils CRM online, Office 365 et Power BI pour ses solutions qui sont aujourd'hui disponibles sur le Cloud de Microsoft.



Une vue de Gigjam qui permet d'intégrer applications et données par de simples gestes comme un rond sur différents documents.

Dominique Gire, un des fondateurs de l'entreprise, rappelle que l'infrastructure peut être un réel handicap dans les projets et que c'est souvent une des causes d'échecs des projets.

Actuellement, Novulys se spécialise sur la relation client, la BI et les analyses sur le Big Data. Cela lui réussi plutôt bien avec des jolis gains de projets d'importance dont certains sur Salesforce.com au cours de l'année. Dominique Gire énumère les avantages que le Cloud lui apporte dans ses discussions avec les clients : *« Nous parlons directement avec les métiers et les fonctionnalités dont ils ont besoin. Les gens de l'informatique*

LES ENTREPRISES EN DEMANDE DE PARTENAIRES

Lors de la manifestation, Microsoft a rendu publique une étude d'IDC réalisée pour son compte autour des besoins et des demandes des clients vis-à-vis des partenaires. Si cette étude se limite aux marchés américain et canadien, elle est globalement représentative des attentes que IDC constate sur les autres zones géographiques, dont l'Europe de l'Ouest.

Principal enseignement de l'étude : 86 % des entreprises souhaitent passer par des partenaires pour acheter, non pas parce que les prix obtenus sont bien meilleurs, mais parce que le partenaire est souvent un partenaire de longue date du client et qu'il sert de conseil technologique auquel l'entreprise fait confiance.

Pas moins de 72 % des entreprises interrogées sont prêtes à payer un supplément pour un meilleur service.

D'autre part, le partenaire est souvent vu comme celui qui connaît bien l'entreprise et son métier, souvent bien mieux que l'éditeur lui-même. Il est vu aussi comme celui qui simplifie la technique et qui aide à bouger vers de nouveaux environnements comme le Cloud. Ce secteur va être un des plus dynamiques dans l'industrie avec une croissance cinq fois plus rapide que l'informatique dite traditionnelle. Il devrait en 2020 représenter près de 40 % des investissements informatiques alors que les autres secteurs resteront à un niveau connaissant à peine la croissance.

Près de 80 % des entreprises interrogées dans l'étude se disaient intéressées par une utilisation dans le Cloud et 70 % des DSI développent une stratégie mettant le choix du Cloud en premier, et en particulier une utilisation d'un Cloud public. La cause de cet engouement ? 72 % des ETI et PME se disent insatisfaites des technologies qu'elles utilisent actuellement. Cette insatisfaction est surtout le fait des lignes de métiers qui jouent un rôle de plus en plus important dans la prise de décision. Près d'une sur trois prévoient des budgets pour un recours au Cloud ou à des services d'hébergement et elles sont beaucoup plus sensibles que le service informatique aux sirènes des services en ligne.

Les entreprises interrogées privilégient d'abord l'expérience commune avec le partenaire dans le choix des solutions, de peu devant le bouche à oreille et les moteurs de recherche. Près d'un tiers regardent les réseaux sociaux et la réputation de la solution ou du partenaire légèrement plus que les rencontres physiques avec le partenaire ou l'éditeur. D'où le fait que 65 % des clients savent ce qu'ils veulent avant d'acheter le produit.

L'étude démontre l'importance du réseau de partenaires pour un industriel de l'informatique et Darren Billy, vice-président, en charge des recherches sur les réseaux d'alliances et de partenaires, de conclure que si un client ne vient pas du fait d'un partenaire, il peut aller voir ailleurs à cause d'un partenaire !

NETGEAR®

Vous faites beaucoup de choses en 1h ...

Gardez un œil sur l'essentiel, en protégeant vos données, toutes les heures !

- ReadyNAS protège vos données avec des **snapshots* toutes les heures,** sans impact sur les performances
- ReadyNAS **s'adapte et évolue** en fonction de vos besoins de stockage
- ReadyNAS est **accessible à distance**, y compris depuis vos périphériques mobiles
- ReadyNAS sécurise votre investissement grâce à **sa garantie de 5 ans avec remplacement en J+1**

Snapshots* illimités | Support virtualisation | Cloud privé et sécurisé | Accès distant | 5 niveaux de protection des données

* Les snapshots sont des points de restauration qui permettent de récupérer n'importe quelle version d'un fichier ou d'une VM (machine virtuelle) avant une modification, une attaque virale, une corruption, un effacement accidentel

Service commercial et avant vente 01 39 23 98 50

www.netgear.fr

préfèrent souvent les environnements Microsoft avec un écosystème riche et largement documenté ce qui leur permet d'être rassurés». Pour lui, le Cloud devient un accélérateur. Les produits et solutions de Novulys ont pour point commun de masquer la relative complexité de l'environnement de Microsoft, en particulier du côté client (mobile, hybride ou sur site) dans les trois domaines ou travaille son entreprise. Il note d'ailleurs que, bien souvent *«les clients sont étonnés lorsqu'on leur montre tout ce qu'ils peuvent faire avec Power BI»*. Lors de notre rencontre, nous avons évoqué les nouveautés présentées lors de la conférence. Si Dominique Gire s'est dit *bluffé* par la démonstration sur Hololens, il considère que le discours tenu par les dirigeants de Microsoft se situe dans une continuité.

45 millions de téléchargement PHP!

Alterway affiche un profil tout à fait différent, et nos lecteurs le connaissent bien, mais sur les environnements… Open Source. Depuis quelques mois, Alterway change son business model et se tourne vers la production (Run) pour ses clients afin de se diversifier et de profiter des opportunités autour du Cloud public dont le prix devient attractif. Pour les interlocuteurs chez Alterway, il y a de plus une véritable place à prendre au regard des 45 millions de téléchargements de PHP sur Windows. Le choix d'Azure était donc naturel et de nombreux clients le demande, nous ont confirmé nos interlocuteurs chez Alterway. L'entreprise a d'ailleurs été primée partenaire mondial pour l'Open Source sur Azure. D'ores et déjà, près d'un quart des machines virtuelles déployées sous Azure l'est sur Linux. ✖

BERTRAND GARÉ

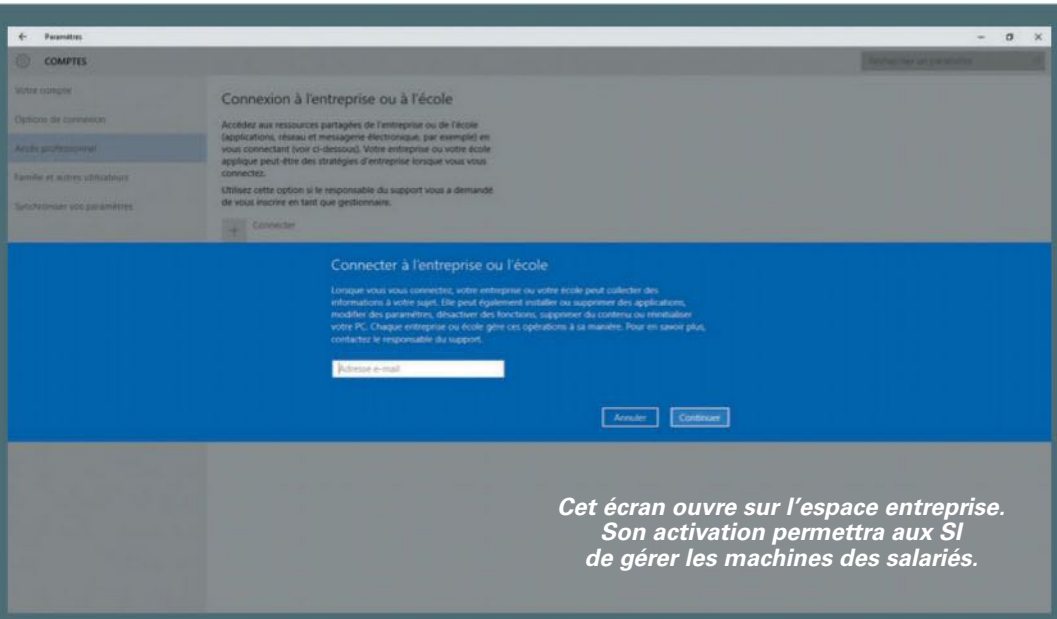
WINDOWS 10 EN ENTREPRISE

Vous n'êtes pas sans savoir que la version finale de Windows 10 a été lancée le 29 juillet. À partir d'un Windows 7 ou du 8, la mise à niveau est gratuite. Les autres utilisateurs devront mettre la main au portefeuille pour migrer vers le nouveau système d'exploitation de l'éditeur. Pour information, une licence Windows 10 Pro est facturée 279 dollars pour une version boîte.

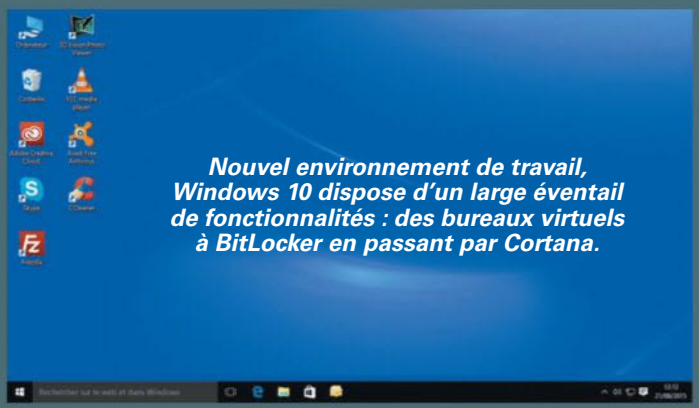
Destinée aux PME, cette déclinaison reprend l'ensemble des fonctionnalités de la version Home (Cortana, Edge, interface…), lui ajoutant quelques options professionnelles. Il s'agit notamment de fonctionnalités de sécurité, avec BitLocker ou encore le démarrage sécurisé, et de gestion d'appareils, en passant par le Business Store pour le déploiement d'applications et Windows Update for Business pour des mises à jour contrôlées. Rappelons que cette variante professionnelle de Windows Update offre à l'utilisateur la possibilité de décider de la fréquence des mises à jour, de les effectuer en peer-to-peer, etc.

Ces deux plates-formes sont également présentes dans Windows 10 Enterprise, le pendant grands comptes de Windows 10 Pro. Les fonctionnalités de MDM et de protection des données à caractère sensible sont plus avancées. On citera, par exemple, Direct Access, AppLocker ou encore Device Guard et Credential Guard. Tout est fait pour réduire la charge administrative des SI et renforcer le contrôle des flottes d'appareils pour une entreprise, notamment si celle-ci a choisi le BYOD. La version Enterprise est disponible depuis le 1er août, payante même si l'entreprise disposait déjà d'une licence sur un des OS précédents.

G. P.



Cet écran ouvre sur l'espace entreprise. Son activation permettra aux SI de gérer les machines des salariés.



Nouvel environnement de travail, Windows 10 dispose d'un large éventail de fonctionnalités : des bureaux virtuels à BitLocker en passant par Cortana.

Kensington

Faites confiance à Kensington. Innovateurs et créateurs de sécurité.

L'ORIGINAL, PAS LA COPIE.

Kensington, la référence pour sécuriser votre matériel depuis 1981.

Contactez-nous :
www.kensington.com/securite

Câble de sécurité mobile MiniSaver™
K67890WW

No.1

N°1 mondial des câbles de sécurité pour ordinateurs portables

Plus de 30 ans d'expérience

Clé passe – L'utilisateur a son propre jeu de clés et un passe ouvre tous les câbles

Clé unique – Un seul jeu de clés ouvre tous les câbles

Clés identiques - chaque clé ouvre tous les câbles

Câbles à combinaison passe ou prédéfinie

Register & Retrieve

Le portail d'enregistrement des câbles Kensington permet aux administrateurs de gérer facilement leur parc d'antivols et aux utilisateurs de bénéficier des services d'assistance Kensington sans dépendre de l'administrateur.

smart. safe. simple.™

« Les systèmes de demain doivent être beaucoup plus prédictifs »

Alex Dayon

Président Produits - Salesforce.com

Serial entrepreneur après avoir dirigé 10 ans la R&D de Business Objects, Alex Dayon est aujourd'hui l'un des principaux dirigeants de Salesforce.com. Il est en charge de l'ensemble de la stratégie Produits. Rencontre avec un personnage totalement immergé dans la culture américaine mais qui n'a rien oublié de ses racines françaises.

L'Informaticien : L'uberisation de l'économie est quelque chose dont on parle de plus en plus. Ne craignez-vous pas d'en être victime à votre tour ?

Alex Dayon : Tout business, y compris celui de Salesforce, peut être « uberisé » et mon métier en tant que patron Technologie est de vivre dans cette paranoïa. Parce que les vagues technologiques évoluent tellement vite. Le Cloud a été une rupture très grande qui a complètement transformé le monde du CRM. Et il va se passer la même chose pour le monde de l'analytics. Et à un moment donné la situation sera identique dans le monde de l'ERP. D'ailleurs, on commence à le voir dans les résultats d'Oracle ou de SAP. Il suffit de lire les données financières pour constater que le scénario est relativement clair.

Vous suivez donc attentivement les évolutions de vos concurrents ?

A. D. : Il faut toujours être attentif aux ruptures de l'industrie. Chez Salesforce, nous passons beaucoup de temps à regarder nos compétiteurs mais ce ne sont pas eux qui nous inquiètent. On vit dans la paranoïa suivante : quelle est la start-up qui va nous uberiser ou tenter de le faire. Donc nous sommes en permanence en train d'acheter de petites sociétés ou de recruter les meilleurs talents car notre offre de valeur est d'aider nos clients dans cette transformation digitale. Les gens qui viennent sur nos événements ne viennent pas pour parler de base de données, de SQL ou de HTML version 5. Ils viennent pour parler de transformation digitale, de nouveaux business models, que ce soit la SNCF ou d'autres très grandes entreprises, tout comme des PME, qui viennent pour comprendre comment transformer une expérience client, comment créer un avantage compétitif, comment être plus productif avec une infrastructure scalable, sécurisée. Tout en s'affranchissant des contraintes technologiques.

Tout comme Meg Whitman, qui dirige HP, vous estimez que le Cloud est le facteur de transformation des entreprises le plus important. De quelle manière ?

A. D. : On a déjà eu ces cinq dernières années des ruptures fondamentales avec la mobilité, la collaboration qui ont transformé radicalement les applicatifs de l'entreprise. Et le Cloud est un catalyseur important pour amener les clients à s'interroger sur la nature de leur système d'information.

C'est là l'un des grands éléments de rupture de Salesforce. Au cours des dix dernières années, avec les réseaux sociaux, les sites web, les applis mobiles, les clients sont devenus partie prenante de votre système d'information. Les clients sont des utilisateurs de votre SI, quel que soit le type d'entreprise. Et c'est là où le Cloud devient vraiment le modèle opératoire pour un applicatif. En effet, vous ne pouvez pas faire connecter votre client à un système à l'intérieur de votre entreprise mais vous devez être entre vos clients et c'est le cœur de la vision de Salesforce depuis le début. Nous ne sommes pas dans le Cloud pour faire la même chose que les autres et être

moins cher. La vraie question est : que pouvez-vous faire avec le Cloud que vous ne pouviez pas réaliser précédemment ?

De quelle manière s'effectue cette évolution ?

A. D. : On voit trois couches successives. Dans un premier temps, les systèmes de données qui sont des SGBD avec du business process. Cela existe depuis plus de vingt ans. Depuis quatre ans a été rajoutée la couche collaborative, ce que l'on nomme en anglais les « systems of engagement ». C'est un process intégré qui connecte les employés, les partenaires, les clients. Cela s'appuie sur des business process des données cités ci-dessus.
La troisième vague qui arrive aujourd'hui est le « system of intelligence ». On va générer des tonnes de données, transactionnelles, collaboratives. Elles sont très importantes. Ce qui fait un bon système décisionnel, c'est le nombre de données et la capacité à les analyser. Les systèmes de demain doivent être beaucoup plus prédictifs, être capables de résoudre des problèmes de manière autonome. Ils doivent permettre aux clients d'avoir plus d'informations de valeur.

Cela veut dire plus de connecteurs vers des applications qui ne sont pas Salesforce, les réseaux sociaux, par exemple ?

A. D. : Il faut être capable d'utiliser ces données à bon escient. Et notre travail est de mettre ces données dans un modèle qui va créer de la valeur pour l'entreprise. C'est avec cela à l'esprit que nous avons racheté relateIQ.com. C'est une technologie à destination des PME. On peut tester des produits de rupture. C'est un exemple très concret des trois couches dont je parlais. C'est une entreprise avec de très forts talents, ils sont tous ingénieurs de Stanford et cela préfigure les applicatifs de demain. Pour nous, c'est la prochaine vague.

Vous venez de sortir une application Analytics qui fonctionne sur l'Apple Watch. Quel est l'objectif ?

A. D. : Avec l'analytics, on avance au fur et à mesure. Et les perspectives sont fascinantes. La montre Watch nous fait comprendre que pour avoir du sens sur ces devices il faut que le backend soit intelligent. Le service cloud doit être très intelligent. La montre est un bon terrain d'expérimentation car cela force à simplifier l'interface.

« Permettre aux clients d'avoir plus d'informations de valeur »

Si vous êtes bon sur une montre, vous serez bon sur un autre périphérique. La montre n'est pas la réponse à tout mais nous sommes fiers car nous avons réussi à faire un produit très pur en termes d'architecture et très simple d'utilisation. Songez que l'on peut explorer toutes ces données avec seulement cinq boutons. De ce point de vue, la volonté d'Apple de simplifier au maximum nous oblige au même effort. Et c'est bénéfique pour tout le monde.

Que pensez-vous de la French Tech et des opportunités des entreprises françaises dans le monde de l'IT ?

A. D. : C'est bien. Il y a de *super boîtes*. La France est pleine de sociétés fantastiques. On a des entreprises très traditionnelles et pourtant très disruptives, et également ces nouvelles entreprises dans l'objet connecté. Ce qui est important dans la French Tech, c'est de rendre la

fierté aux entrepreneurs. La France a un système éducatif fantastique et une volonté de faire des choses. C'est un pays de qualité également.

Dans ces conditions, croyez-vous que la France dispose de tous les atouts pour qu'une entreprise française soit le prochain Google ou le prochain Salesforce ?

A. D. : Cela sera encore dur. Pour plusieurs raisons. La première, c'est le financement. Il n'y a pas les structures adaptées. Cela fonctionne pour les phases initiales mais pas pour les phases suivantes. Les second et troisième tours. On a réglé les problèmes d'amorçage mais les problèmes surviennent plus tard. Aujourd'hui les tickets d'entrée sont élevés. Quand on voit ce qui est mis dans la Silicon Valley, personne en Europe ne peut suivre. Attention cela ne veut pas dire que la Silicon Valley est raisonnable et qu'il n'y aura pas de retours de bâton, mais clairement il faut être capable de travailler à l'échelle européenne a minima.

Ensuite il faut savoir « exécuter » aux États-Unis compte tenu de la taille du marché. Les entreprises ne doivent avoir ni honte, ni inquiétude dans l'exécution sur ce marché. Cela doit faire partie du modèle. Les Français doivent s'intégrer dans le paysage américain et savoir opérer sur ce marché. C'est tout à fait possible aujourd'hui.

Voyez-vous une nouvelle consolidation parmi les acteurs du Cloud ou de l'Hadoop ?

A. D. : Il y a une telle phase d'innovation que cela suscite de la compétition et les acteurs cherchent à s'offrir les meilleures entreprises. Toutefois, les capitalisations sont tellement élevées que cela ralentit le processus. Mais si les marchés baissent, cela offrira des opportunités. Les tours de table sont entre *100 et 200 millions* au minimum. Il faut avoir les reins solides pour suivre et, une nouvelle fois, l'Europe n'est pas encore prête dans ce domaine.✖

Propos recueillis par Stéphane Larcher

« Les Français doivent s'intégrer dans le paysage américain et savoir opérer sur ce marché. C'est tout à fait possible aujourd'hui »

airwatch by vmware

Déployer du BYOD sans compromettre la sécurité

AirWatch offre une plateforme flexible conçue pour sécuriser les terminaux mobiles appartenant à l'entreprise ou à l'employé, protéger les données professionnelles et personnelles, sécuriser l'accès aux ressources d'entreprise, aux applications et aux documents et assurer leur conformité.

À propos d'AirWatch by VMware

AirWatch by VMware est leader de la gestion de la mobilité d'entreprise. La plateforme AirWatch offre les meilleures solutions de gestion des terminaux mobiles, des e-mails, des applications, du contenu et de la navigation. Acquis en février 2014 par VMware, le siège d'AirWatch pour l'EMEA est situé au Royaume-Uni (www.air-watch.com/fr).

sales@air-watch.com | air-watch.com/fr

1ER ÉVÉNEMENT EUROPÉEN
LIBRE & OPEN SOURCE

OPEN FOR INNOVATION

opensourcesummit.paris

#OSSPARIS15

PARIS OPEN SOURCE SUMMIT

18&19 NOVEMBRE

DOCK PULLMAN
Plaine Saint-Denis

PARTENAIRES INSTITUTIONNELS

SPONSORS PLATINUM

SPONSORS GOLD

SPONSORS SILVER

POUR TOUTE INFORMATION COMPLÉMENTAIRE :
Email : contact@opensourcesummit.paris – Tel : 01 41 18 60 52

un événement

Le bullet point de…

Bertrand Garé

Rédacteur en chef

SÉCURITÉ

Prévenir plutôt que guérir

Alors que les attaques et les fuites de données deviennent quasi quotidiennes, les entreprises changent peu leur approche dans le domaine. Se sentant protégées derrière des remparts hardware, elles oublient que le meilleur remède est souvent de se préparer à l'attaque et non seulement de chercher à réagir lorsqu'elle survient.

Inconscience ou véritable sentiment de sécurité ? 85 % des salariés français pensent que leur entreprise est bien protégée et seulement un tiers d'entre eux croit que leur entreprise a été attaquée. La réalité est tout autre et, selon Cap Gemini, ce sont bien 90 % des entreprises françaises qui ont subi des attaques dans les derniers mois. Pour se rendre compte de l'ampleur du phénomène, l'administration fiscale américaine enregistre 145 millions d'attaques par an ! Pas de chance, certaines ont réussi à traverser la carapace et 4 millions de fonctionnaires américains ont vu leurs données dévoilées sur la Toile. Notre pays peut souffrir de la comparaison, l'administration fiscale française ne déplore que 100 000 attaques par jour ! Les grandes administrations ou entreprises ne sont pas les uniques victimes des hackers de tous poils. Plus de 40 % des PME sont victimes des mêmes impedimenta. Ce chiffre monte à 90 % dans la distribution. Mieux, 90 % des attaques se réalisent sur des anciennes failles que les entreprises n'ont pas corrigées.

Arrêter d'empiler !

Pourtant des solutions pour se défendre, les entreprises en ont. C'est même un des secteurs les plus dynamiques dans l'industrie informatique. Évidemment, si ces éléments ne sont pas à jour, c'est de l'argent jeté par les fenêtres grandes ouvertes de votre entreprise. Les entreprises empilent de merveilleuses machines technologiques pour *« avoir une défense de bout en bout »*, mais rarement intégrées entre elles laissant béants des espaces ou permettant d'augmenter la surface d'attaque pour les hackers. Pour preuve, Kaspersky Labs a été victime d'une intrusion sur ses serveurs. Le message est clair : personne n'est à l'abri et la bonne question à se poser n'est pas de simplement s'inquiéter mais de savoir quand aura lieu l'attaque et donc de s'y préparer au mieux. Pourtant, l'ANSSI vient de rappeler récemment qu'avec des mesures simples, mais réellement appliquées, 95 % des attaques pourraient être évitées.

Un sentiment de Ligne Maginot

Comme dans les années 40, les entreprises se défendent des menaces de la guerre d'avant avec une vision de ligne Maginot avec ses structures « en profondeur » et son repli élastique sur

des « *positions préparées à l'avance* », il ne manquerait plus qu'elles nous disent que la route de l'acier est coupée pour que le tableau soit complet. Peu d'entre elles systématisent par exemple la gestion des risques informatiques en dehors de la formalisation pour le rapport annuel ou le respect des conformités aux règles législatives. Quelles sont véritablement les données qui doivent être protégées ? Qui peut y avoir accès ? Dans quelles conditions ? Qui est responsable de la mise à jour des éléments entrant dans la sécurité ? Des évidences direz-vous mais encore faut-il que ce travail soit fait et maintenu dans le temps.

L'ennemi intérieur

Autre erreur stratégique, la plupart des attaques spectaculaires proviennent d'utilisateurs internes, que ce soit par vol d'identité via phishing ou par malveillance. Or, la plupart des solutions de sécurité conservent une vision où le gentil est à l'intérieur et le méchant hors les casemates de la ligne Maginot. Sans vouloir reprendre une affiche célèbre des années de la drôle de Guerre, indiquant que les murs ont des oreilles et que la « cinquième colonne » nous écoutait – on sait maintenant que même nos amis le font ! –, l'appel à la vigilance des salariés est un minimum. Certaines initiatives récentes semblent assez bienvenues. Ainsi, Cap Gemini va intégrer 68 règles de conduite relatives à la sécurité informatique dans son contrat de travail. Si la méthode douce ne fonctionne pas, alors essayons cela ! Le Cigref propose, lui, un jeu « un serious game », pour que les salariés se forment aux règles élémentaires de la sécurité. D'après les premiers retours, l'adoption est intéressante et les salariés comprennent enfin pourquoi on leur demande telle ou telle chose dans leur travail quotidien. L'exemple du changement et de la gestion des mots de passe dans les entreprises en est le point le plus intéressant, vu du côté de l'utilisateur comme le pensum de la sécurité mais qui reste le premier bouclier contre les intrusions.

Rester pragmatique

Cette complexité des procédures de sécurité dans le travail quotidien encourage les comportements déviants et l'informatique cachée. Expliquer et rester simple dans l'application des règles de sécurité, savoir gérer les exceptions pour éviter les situations ubuesques où le salarié doit demander trois autorisations pour avoir accès à un contenu ou une application dont il a besoin dans son travail… Eh si, je vous assure cela existe. Il est aussi possible de revoir la conception des fameuses chartes informatiques que tout le monde a lu en entrant dans l'entreprise mais qui n'est que rarement appliquée car les exceptions constatées chaque jour font que le texte est inepte. Il est peut-être nécessaire de rappeler que ce texte s'impose normalement à tous, du PDG de l'entreprise au plus simple des salariés, et que l'exemple vient souvent du haut !

Mobiliser les ressources nécessaires

Faut-il rappeler que la détection d'attaques et la mise en place de plans de réponse demandent d'avoir des gens formés et spécialisés disposant de l'outillage adéquat. La mise en place de la politique de sécurité permet en premier lieu de suivre les bonnes pratiques qui limiteront les dégâts lors d'une attaque, mais aussi de sauvegarder les preuves de l'intrusion pour au moins pouvoir porter plainte. Trop souvent, pour éviter les premiers symptômes de l'attaque, la réponse est, hélas !, de prendre des mesures qui ne permettent plus d'avoir les éléments constitutifs de l'attaque. Organisation, culture différente voilà peut-être ce que demande la sécurité et non pas encore plus d'outillage. En vous souhaitant une bonne rentrée, vu le travail à faire dans le domaine ! ✖

Bertrand Garé

COMMENTER, RÉAGIR, PARTAGER…

dans la rubrique *Débats* de linformaticien.com

DÉVELOPPEMENT PROFESSIONNEL

WINDOWS, LINUX, IOS, ANDROID, CE, WEB...

100 TEMOIGNAGES DE SOCIÉTÉS PRESTIGIEUSES, C'EST UTILE !

Philips, VINCI Autoroutes, Quick, Système U, Fédération Française de Basket-Ball, Bolloré Africa, Casio, Taittinger, CCI de Bordeaux, VOLVO Car France, AIGLE, Siemens VAI, Truffaut, Air Calédonie, HONDA, Comtesse du Barry, Ministère de l'Education Nationale, Ecole d'ingénieurs de Paris, EcoleDirecte.com, Isotoner, Hôpitaux de Paris, Autosur, Société Générale, Photomaton®, Groupama, ...

Vos clients, vos utilisateurs ont besoin de solutions rapides et fiables, dans tous les environnements, sur tous les matériels.

Quoi de mieux qu'un AGL-ALM **compatible avec tous les systèmes et tous les matériels**?

Nous sommes heureux de vous offrir ce numéro spécial publi-dossier de la revue **01 Net** présentant **140 pages de témoignages dans tous les domaines (applications stratégiques, applications départementales, sites Internet et Intranet, applications mobiles)...**, sur tous les matériels.

Découvrez ce que **WINDEV** vous apporte, et apporte à vos utilisateurs et clients.

Vous ne vous satisfaites pas des simples messages commerciaux, bien entendu. C'est pour cela que ces 140 pages de témoignages récents vous permettent de vous forger **votre propre avis**.

Disponible en **lecture libre sur le site www.pcsoft.fr**, ou sur votre bureau demain (offre d'envoi gratuit réservée aux professionnels).

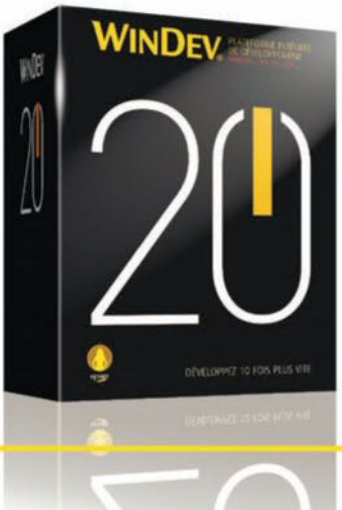
WINDEV :
UN TAUX DE SUCCÈS DES PROJETS SANS ÉQUIVALENT

Logiciel professionnel.

WINDEV®

WINDEV AGL N°1 en FRANCE

Fournisseur Officiel de la Préparation Olympique

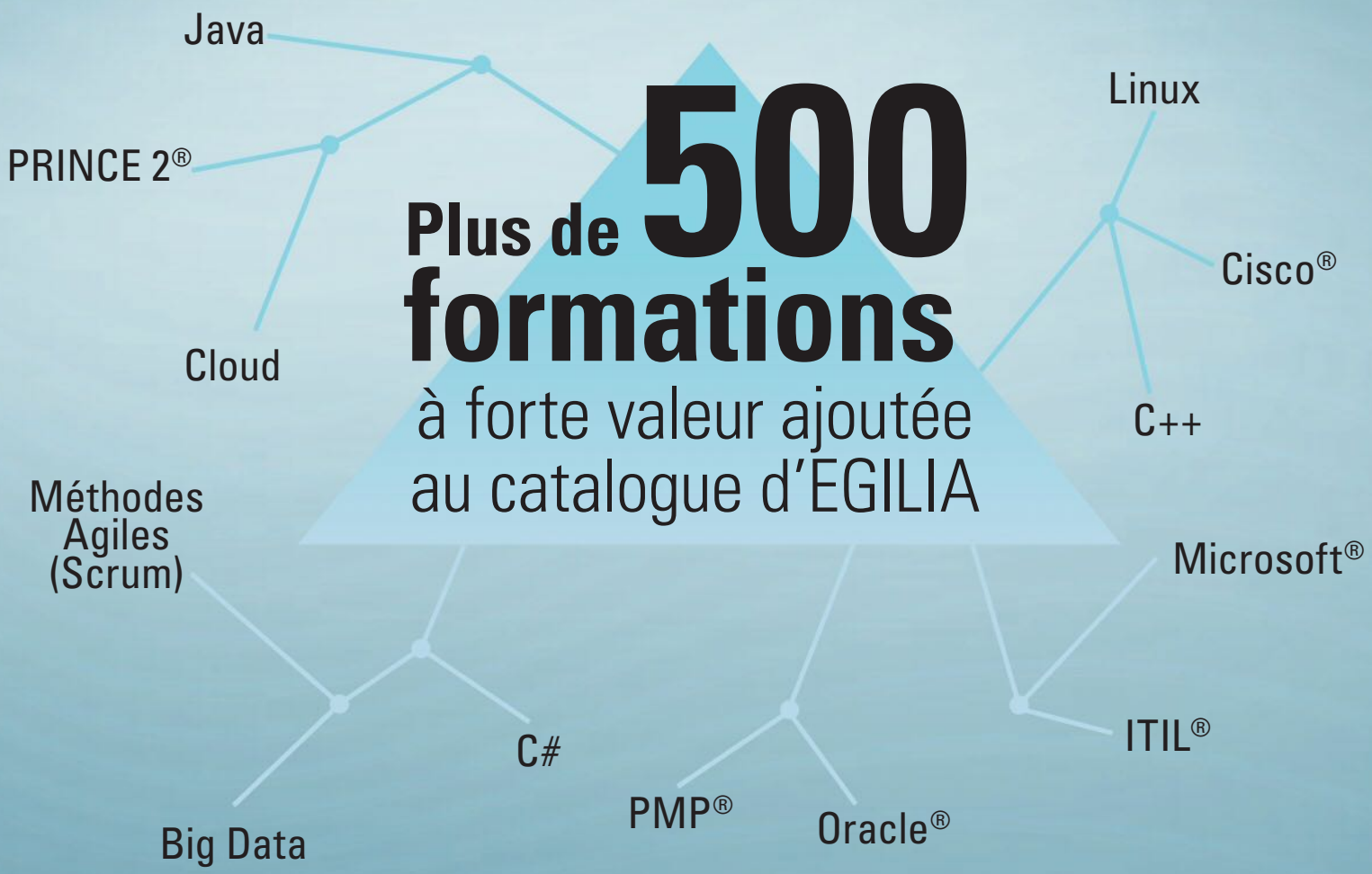


www.pcsoft.fr

egilia® & L'INFORMATICIEN
www.linformaticien.com

offrent 1 an d'abonnement aux participants des formations EGILIA

EGILIA, le spécialiste de la formation certifiante en informatique et management, et **L'Informaticien,** proposent désormais, pour chaque inscription à une formation certifiante **EGILIA,** un abonnement d'un an à **L'Informaticien** en version numérique + newsletter.



Nos conseillers sont à votre écoute : 0800 800 900 (appel gratuit depuis un poste fixe).
Retrouvez nos formations sur notre site : www.egilia.com

ITPT Silicon Valley,

SDN, Flash et Open Source

Le dernier IT Press Tour (ITPT) a démontré certaines tendances fortes dans différents secteurs, dont le réseau et l'infrastructure. Également mis en avant : le Software Defined Networking, l'omniprésence de Flash dans le stockage et de nombreuses innovations dans des projets Open Source, des containers aux bases de données en passant par l'analytique.

Alex Bouzari, chez Data Direct Network (DDN), vit à Los Angeles pour ne pas être dans *« la Vallée qui ne se préoccupe que des dernières tendances de l'IT, omniprésente là-bas, et donc pas forcément l'endroit idéal si on ne veut pas être intoxiqué par les modes du moment »*. Patron de l'entreprise de stockage, Alex Bouzari préfère écouter ses clients et ses partenaires que les derniers gourous en date. Pour les lecteurs de *L'Informaticien*, c'est un peu différent. Alors…, que nous mijotent les entreprises de la Silicon Valley ?

La virtualisation s'étend au réseau

Nous avions bien visé en vous proposant dernièrement un dossier sur un des sujets les plus chauds du moment, le Software Defined Networking (cf. notre numéro de juin 2015). Aux États-Unis, le sujet est réellement sur le devant de la scène avec l'annonce d'AT&T, premier opérateur de télécommunications américain, de vouloir virtualiser 75 % de ses services dans les cinq ans. La question n'est plus de s'interroger sur la technologie et ses avantages, mais bien de la déployer dans les mois à venir. Lors de notre périple nous avons rencontré deux acteurs du secteur, Big Switch et Nuage Networks. Les deux proposent des solutions sensiblement différentes.

Big Switch a été créé en 2010 et compte au sein de son conseil d'administration Michael Dell et Vinod Khosla, l'un des fondateurs de Sun et l'un des plus gros Venture Capitalist de la Silicon Valley. Le signe distinctif du dernier nommé ? Il ne se trompe que très rarement dans ses investissements, et son soutien est très recherché car il peut ouvrir de nombreuses portes ! Les autres membres du board sont du même calibre avec des anciens de chez Cisco, Juniper, McKinsey… L'entreprise a levé jusqu'à maintenant 47 M$. Cet acteur souhaite désormais viser le marché européen au cours du premier trimestre de l'année prochaine.

Pour Big Switch, l'architecture traditionnelle des réseaux ne peut soutenir la demande actuelle et à venir dans les centres de données et induit une complexité d'administration du fait d'un management équipement par équipement. L'entreprise américaine veut sortir de ce schéma en proposant une architecture qui repose sur trois principes : la topologie de Clos, (un switching cross bar, issu des travaux d'un chercheur des Bell Labs dans les années 50 sur le switching non bloquant pour les appels téléphoniques), l'utilisation de matériels de commodités et un contrôle centralisé.

Alex Bouzari, CEO de DDN.

L'étape suivante est de réutiliser ces principes pour les étendre au campus puis au WAN (Wide Area Network). Il est à noter qu'avec leur implémentation TRILL (Transparent InterConnect of a Lot of Links) la plupart des offreurs de switches sur le marché proposent ce type de topologie comme Cisco, Juniper, Brocade et Arista. Le déploiement se réalise sur des environnements « Bare Metal » pour proposer un SDN ouvert s'inspirant pour beaucoup de l'architecture du projet Jupiter de Google pour la virtualisation de réseau. Celui-ci a été présenté le 17 juin dernier lors de l'Open Networking Summit qui s'est tenu à Santa Clara. Jupiter utilise Open Flow.

À l'image de ce que la virtualisation a réalisé dans les environnements serveur, en désintégrant les mainframes avec des systèmes x86, Big Switch veut désintégrer le « Netframe » en proposant pour le réseau des possibilités de « scale out » pour les réseaux avec un point de contrôle sur le niveau spine du réseau. Intégré avec vSphere de VMware, la solution se place en sous-jacent de NSX-V.

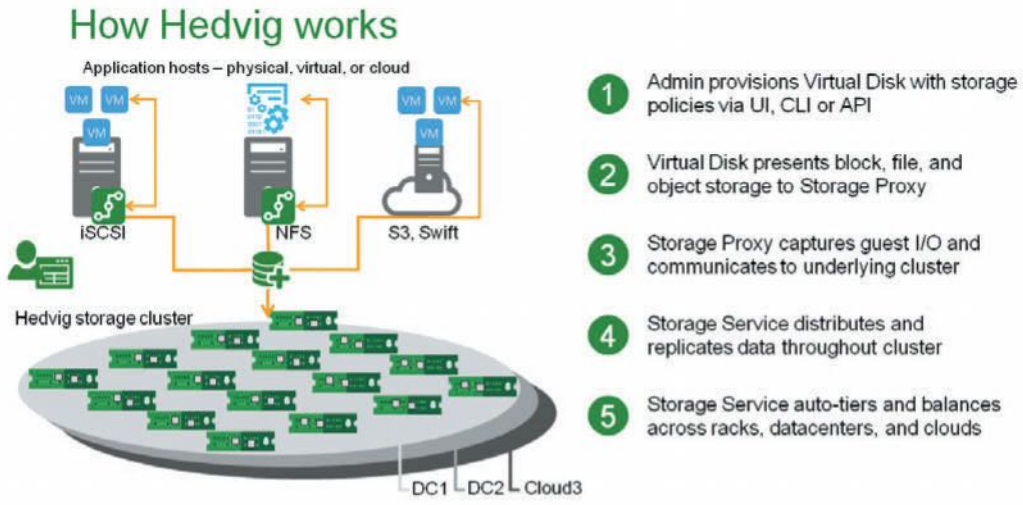
640 pannes forcées

Un des avantages de l'architecture proposée est sa résistance aux pannes 640 composants peuvent tomber en une demi-heure sans qu'il n'y ait d'impact sur l'application utilisée, démonstration faite lors d'un « Chaos Monkey Testing » avec 42 000 machines virtuelles et plus de 640 pannes forcées lors du test. Au niveau du contrôleur, le failover était de 30 secondes, de 8 secondes au niveau du switch et de 4 secondes au niveau du lien. La solution embarque son propre reporting et le support d'Open Stack.

Nuage Networks, une spin-off d'Alcatel-Lucent, présente une autre approche du SDN avec la création d'une couche d'abstraction et d'automatisation entre les fonctions réseau et les équipements hardware. La solution fonctionne selon des règles métier et non les protocoles utilisés. Nuage Networks part du constat que le réseau n'est plus la ressource réellement demandée mais bien l'accès et l'utilisation des applications, ce qui induit la nouvelle approche SDN du réseau. Avec la plate-forme de Nuage Networks, les propriétés réseau adéquates sont propagées aux différentes charges de travail, quelles que soient les infrastructures ou la localisation géographique. Les équipements hardware sont juste utilisés pour le transport, l'automatisation et le plan de contrôle sont placés dans un switch virtuel qui crée les tunnels sécurisés (VxLAN) suivant les règles métier de chaque charge de travail. Des clients comme les banques espagnoles BBVA ou Santander utilisent la plate-forme.

Flash s'impose sous toutes ses formes

Comme toujours, une large partie de nos visites était consacrée à des entreprises dans le secteur du stockage. Point commun dans toutes ces entreprises, la présence de la technologie Flash que ce soit à 100 % ou dans des environnements hybrides. Issue des environnements HPC, la solution de Data Direct Network (DDN) vise les environnements très haut de gamme ou demandant des performances quasi extrêmes comme dans la finance ou le secteur de l'énergie du fait de la vitesse et du volume de données à traiter. DDN s'appuie sur des solutions convergentes et hyper-convergentes sur des disques Flashs pour proposer des scenarios de stockage allant de la mémoire jusqu'au Cloud en passant par les disques classiques ou les bandes. Le pari, comme l'indique Alex Bouzari, le CEO de DDN, est que *« les entreprises choisissent toujours la fiabilité sur la performance »*. Cela n'empêche pas d'offrir des performances que peu de matériels peuvent atteindre sur le marché avec la capacité de traiter 5 millions d'IOPS dans un châssis de 4U avec la possibilité de supporter 100 000 machines virtuelles. Le portefeuille de produit de DDN permet de traiter



Le mode de fonctionnement d'Hedvig.

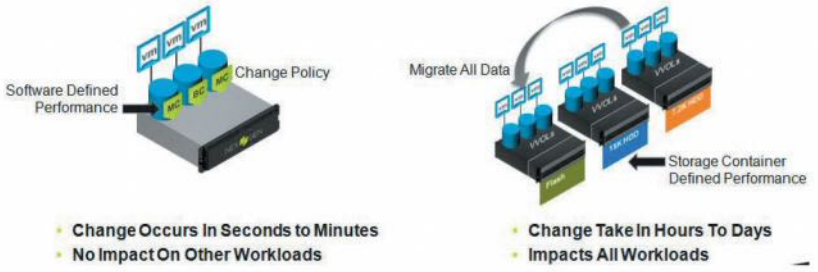
tous les types de données. Wolfcreek, le nom de la plate-forme, supporte de plus Hadoop et Open Stack. La solution se présente sous la forme d'une appliance 4U ou en appliance virtuelle sur n'importe quel hardware de commodité x86. Un moteur en mémoire sert d'accélérateur pour le traitement des I/O.

Autre annonce importante de l'éditeur : DDN se lance dans les environnements objets avec WOS 360. La solution est disponible depuis le 30 juin. Là encore les performances sont impressionnantes et visent évidemment les larges environnements du Web. Pour Alex Bouzari, les types d'architecture inspirées du Web vont devenir *« de plus en plus fréquentes dans les entreprises. Notre plate-forme se veut être la passerelle entre ces deux mondes, qui ne se sont pas encore totalement rejoints »*.

Des serveurs ARM avec du Flash

Hedvig, une des nouvelles entreprises dans le stockage qui commence à réellement faire parler d'elle au-delà de la Silicon Valley, se sert des mêmes sources d'inspiration, les environnements des grands faiseurs de l'Internet. Avinash Lakshman, CEO et fondateur d'Hedvig, ajoute : *« Le modèle de demain pour les grands du Net est de s'appuyer sur des serveurs ARM avec du Flash. On en n'est pas encore là dans les entreprises. »* Pour lui, dans le stockage, il n'y a pas eu d'innovations fondamentales depuis dix ans. Techniquement Hedvig propose une solution de stockage distribué par logiciel sur des matériels peu chers. Sous cette forme virtuelle, la solution peut évoluer quasiment linéairement par simple ajouts de nœuds pour stocker des Petaoctets de données sur tous les protocoles, blocs, fichiers ou objets, dans n'importe quel environnement – Clouds public/privé ou sur site. La plate-forme se compose d'une couche de service de stockage qui s'occupe du maintien en condition opérationnelle des clusters et d'un moteur distribué qui gère les fonctions avancées de stockage et les remédiations en cas d'incidents. Un proxy de stockage présente les éléments de stockage (blocs, fichiers, objets) via une machine virtuelle à l'environnement de stockage ou à un container de type Docker. Des disques virtuels fournissent une couche d'abstraction pour un provisioning fin des fonctions de stockage dans l'entreprise.

Autre star du Flash, Pure Storage est revenu lors de notre visite sur ses annonces récentes autour de Flash Array M, Pure 1 et Evergreen Storage. Flash Array M propose une baie optimisée supportant 120 Téraoctets dans 3 U pour une consommation de 1 KW, soit une amélioration significative de la densité et de la consommation sur les matériels antérieurs ou les principaux concurrents du marché. La solution se présente dans trois configurations, M20/50/70. Des mises en production ont eu lieu dès juillet dernier et la disponibilité générale des produits est prévue à la fin de ce trimestre. Pure 1 est une console de gestion du stockage dans le Cloud accessible donc depuis des environnements mobiles. Une petite surprise nous attendait cependant avec l'annonce de l'extension des offres Flash Stack aux environnements SQL de Microsoft et XenDesktop de Citrix.

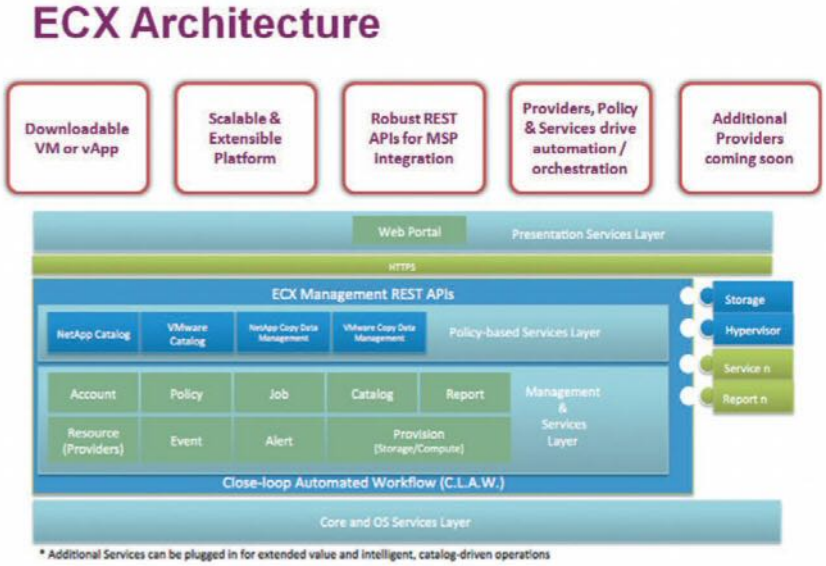


Comment NexGen évite d'utiliser vMotion.

Du Cloud vers l'entreprise

Avere, historiquement dans le monde du NAS (Network Area Storage), étend ses possibilités vers le Cloud. En mars 2014, l'éditeur avait déjà annoncé son support d'Amazon ; cette fois il allie le calcul à sa palette produit avec un stockage fichier virtuel et le snapshot des référentiels d'objets dans le Cloud. Tout ceci s'appuie évidemment sur la technologie Flash. Véritable différenciateur, Avere est le seul actuellement à proposer ces fonctions du Cloud vers le site de l'entreprise. Les autres ne fournissent que des extensions dans le sens entreprise vers Cloud. Les cas d'usages sont assez nombreux et certains sont déjà en production comme une entreprise dans la génomique, une autre dans la production de films

Un peu à côté de ces grandes tendances, NexGen Storage propose sur PCIe une solution de QoS du stockage pour les environnements fortement virtualisés sous VMware. Installé comme un plug-in de vCenter 6, NexGen QoS Manager administre les tâches de stockage via vCenter à partir de règles avec les demandes de capacité de stockage. Celles-ci sont traitées par la couche de contrôle qui expose les capacités demandées et les provisionnent vers l'application ou la



L'architecture d'ECX de Catalogic.

machine virtuelle adéquate. La solution intègre de plus la technologie VVOL de VMware. La maîtrise de la qualité des services se réalise à deux niveaux, celui de la VM ou de l'I/O si nécessaire. Dans certains cas, la solution présente l'avantage d'éviter l'utilisation de vMotion et gère très rapidement les changements demandés dans l'infrastructure de stockage.

Effacer certaines copies de données

Catalogic Software s'attaque à un problème totalement différent et se rapproche plus de la gouvernance des données avec une solution de gestion des copies de données. Selon IDC, 60 % des capacités de stockage sont fagocytées par des copies de données, la plupart inactives et peu intéressantes pour les lignes de métier.
Avec ses logiciels DCX et ECX, Catalogic se propose à la fois de protéger les données mais aussi d'optimiser le cycle et le nombre de copies de données pour libérer de l'espace de stockage, et donc de l'argent pour les entreprises. La solution indexe tous les snaps, les réplications et les objets VMware avec une vision fine du contexte de l'environnement de l'entreprise ainsi que l'héritage des différentes copies et leur localisation dans les serveurs de l'entreprise. La solution permet aussi du reporting sur la conformité vis-à-vis des règles de l'entreprise ou des lois en vigueur. Suivant le nombre de copies, l'environnement peut être nettoyé. Eh oui, les entreprises commencent à découvrir qu'il est possible d'effacer certaines copies de données tout en ne prenant aucun risque légal. Il est aussi possible de transférer les données sur des supports de rétention de long terme peu chers, tout en vidant l'espace de stockage primaire ou secondaire. Cette fonctionnalité de gestion des copies devient un secteur à part entière du stockage avec des acteurs très actifs comme Actifio et très certainement Veritas dans les mois à venir.

Le futur du Flash

Une des visites marquantes de ce tour aura été Micron, un grand nom du monde SSD qui nous a un peu ouvert les portes vers ce que sera le monde Flash de demain. Aujourd'hui déjà existent des disques Flash s'adaptant à tous les types d'environnements selon les besoins en endurance ou en capacité.
Micron parie sur la Technologie NAND et voit le PCIe se développer largement dans les années à venir. Les pistes de travail de Micron tournent autour de trois axes. Le premier est le NAND 3D. Dans son design, les cellules NAND de ces systèmes se présentent comme des gratte-ciels. Ce design permet d'atteindre des densités beaucoup plus importantes qu'auparavant pour des coûts inférieurs à ceux du design en 2D, et ce, pour des performances et une endurance supérieures. Un modèle TLC sur ce design permettrait des disques à 384 Go. Sur ces technologies Flash, Micron veut apporter plus de valeur avec ses solutions de stockage optimisées par charge de travail. Pour cela une pluie d'annonces de produits à venir comme une solution sur PCIe pour accélérer la lecture des données mais aussi le stockage des métadonnées. Dans la même famille, un accélérateur en lecture/écriture sur SAS devrait lui aussi voir le jour rapidement. Pour le stockage dans les centres de données, des composants sur PCIe, SAS et SATA vont suivre. Des produits de ce type devraient aussi être disponibles pour le marché Consumer mais aussi pour les postes de travail en entreprise.

L'Open Source sur le devant de la scène

La Silicon Valley part d'un constat, parfois discutable, selon lequel l'innovation vient aujourd'hui des grands du Web et non plus des acteurs classiques. La plupart de ceux-ci ont mis leurs innovations en Open Source du fait que les produits du marché ne pouvaient répondre à leurs exigences. Ainsi Facebook, Google, LinkedIn, Amazon ont créé leur propre base de données. Basho Technologies se place dans cette lignée avec une base NoSQL avec plusieurs principes affichés comme de

privilégier la résilience plutôt que la possibilité de remédiation. La solution est distribuée pour que chaque composant travaille sur de petites tâches avec la possibilité de faire évoluer la solution linéairement pour la performance, la capacité avec l'idée de « survivre » aux incidents et non plus de réagir aux incidents. Basho se classe dans la famille des bases de données Clés/Valeurs et son architecture n'est pas sans rappeler le Ring de Scality, une base de données objet dans le Cloud. Les Clés/Valeurs sont répliquées trois fois dans l'anneau de serveurs du cluster. Les données restent ainsi disponibles même si plus d'un nœud du cluster tombe. La base de données est très ouverte avec un jeu d'API très large et des kits de développements pour les principaux langages connus dont Go, la dernière coqueluche de la Vallée issue des travaux d'une équipe de Google et de membres de la communauté qui s'y est agrégé. Ce langage est assez proche du C mais le rénove en étant plus concis, en y ajoutant des fonctions intéressantes de relâchement de la mémoire. Sa syntaxe est, de plus, simple. Basho est évidemment bien intégré avec le monde du Big Data et propose des outils qui permettent d'éviter d'utiliser des logiciels comme Zookeeper, une plate-forme d'administration du monde Spark, le nouveau moteur de requête de la stack Hadoop, qui s'impose peu à peu, ou SolR, un moteur de recherche dans les données, assez proche d'Elastic Search.

La santé de l'entreprise par le logiciel

Autre exemple de cette tendance, JUT est une plate-forme en ligne pour ingérer, corréler et analyser toutes les données opérationnelles dans l'entreprise. Steve Mc Canne en est le CEO et fondateur. Ce serial entrepreneur, bien connu dans la Silicon Valley, avait fondé par exemple Riverbed et Fast Forward Networks. Il est aussi professeur à l'Université de Californie sur les technologies réseau. L'entreprise a deux ans d'existence et a déjà levé en deux tours 23 millions de dollars.

Pour Steve Mc Canne, le monde tourne autour du software et, pour comprendre la santé d'une entreprise, il suffit d'avoir l'état de santé de ses logiciels. JUT veut donc fournir la vision globale de cette santé pour comprendre et agir sur les opérations des entreprises. Avec les silos actuels, la solution à ce problème n'est pas triviale. Dans le domaine, les entreprises accumulent les outils, souvent sans lien entre eux et n'ont alors qu'une vision parcellaire de leur organisation informatique. Les corrélations et analyses sont complexes, voire impossibles. JUT veut régler ce problème en proposant une vision globale avec la possibilité de créer les analyses qui sont pertinentes pour l'entreprise. Sur Data Flow, JUT a créé un moteur de données et un langage (Juttle) pour créer les rapports et analyses sur ces données. Des packages et des API spécifiques sont présents pour collecter les données dans des environnements différents comme Hadoop. Pour Mc Canne, *« JUT est un mix entre Google Data flow et ce que peut faire Tableau sur la visualisation »*.

Juttle est un langage de haut niveau déclaratif de script qui permet à l'utilisateur de se concentrer sur la réponse à la question qu'il pose et non sur la question ou la requête elle-même. Ainsi des requêtes en JUT peuvent prendre trois lignes alors que la même requête en Map/Reduce pourrait prendre une centaine de lignes de code. Les compétiteurs de la solution sont multiples, tel que Splunk, Sumologic, Librato ou Spark. Le produit est en Beta ouverte sur le site de JUT. N'hésitez pas à aller « jouer » avec !

Comme les grands du Web

Comme nous le disions en introduction, l'innovation vient des grands du Web. Alors, soyons fou, comment avoir la même infrastructure que ces grands du Web dans votre entreprise ? C'est le pari de CoreOs, une entreprise qui développe Gifee (Google Infrastructure for Everyone Else !). S'appuyant sur les briques rkt et etcd et de nombreux autres projets Open Source, CoreOS a développé une stack. Depuis celle-ci, l'équipe de 40 personnes de San Francisco vise désormais les entreprises avec Tectonic, une solution qui inclut Kubernetes et sa pile logicielle pour une utilisation massive des containers Linux, la toute dernière folie de la Silicon Valley vue comme la véritable alternative aux outils de virtualisation actuels. Cette approche purement Open Source diffère un peu de Docker. De toute manière, les containers de ce type vont connaître de multiples versions car tout le monde développe sa propre vision autour du concept.

Au final, un tour bien intéressant devant la variété des tendances présentes avec une grande ouverture sur les tendances à venir. ✖

Bertrand Garé

Cyberdéfense

Checkmarx veut démocratiser l'analyse du code

Le spécialiste israélien de la sécurité applicative qui marche dans les pas de Veracode et Quotium, tente de s'imposer dans l'analyse du code statique.

Le champion israélien de l'analyse du code statique Checkmarx n'a pas encore mis le cap sur le Nasdaq, à l'instar de son compatriote CyberArk Software. Mais la société a de nouveau prouvé qu'elle avait le vent en poupe auprès des investisseurs. Créée en 2006 par un expert en cyberdéfense, Maty Siman, et dirigée par Emmanuel Benzaquen, un vétéran de la tech d'origine française, l'entreprise avait commencé par s'attirer les grâces du groupe d'investisseurs Ofer High-tech et de Salesforce.com. Elle a annoncé fin juin avoir levé 84 millions de dollars auprès du fonds américain Insight Venture Partners. Et ce, après avoir levé 15 millions de dollars depuis sa création.

Un véritable vote de confiance pour cette société employant 150 salariés répartis entre Israël et les États-Unis. De fait, marchant dans les pas de géants comme Veracode ou Quotium, Checkmarx a su très tôt proposer des solutions visant à dissuader les hackers le plus en amont possible. *« La technologie a évidemment énormément évolué »*, précise Emmanuel Benzaquen, le PDG et responsable de la technologie de l'entreprise, mais le principe reste le même : fournir aux développeurs d'applications, des solutions leur permettant de détecter les phénomènes de vulnérabilité.

Pour ce faire, Checkmarx a mis au point un « moteur de scan » permettant aux utilisateurs de comprendre le comportement du code, et d'identifier les failles possibles que des hackers pourraient mettre à profit pour dérober des données. *« Il y a deux ou trois ans, les développeurs ne se préoccupaient guère de sécurité : historiquement, cela ne faisait pas partie de leurs objectifs »*, poursuit le PDG de la société. Mais à l'heure où des groupes comme Sony ou PayPal ont été la cible de cyberattaques, il est devenu indispensable de mettre en place des solutions de sécurité au niveau applicatif.

Intégrer la dimension comportementale

Fort de quelque 700 clients, dont Coca-Cola et l'armée américaine, Checkmarx dessert aussi bien des établissements bancaires, les télécoms, le monde de l'assurance que des administrations. Labellisée « visionnary player » par le cabinet d'études Gartner, la firme revendique une technologie appartenant à la nouvelle génération. *« On procède à l'audit du code, en intégrant la dimension comportementale »*, confie encore son dirigeant. *« Rien ne sert de sécuriser les réseaux si l'on n'a pas mis en place des garde-fous au niveau applicatif. »*

Présent dans 28 pays, Checkmarx réalise la moitié de son activité aux États-Unis, 30 % en Europe et 20 % en Asie, et investit la moitié de son chiffre d'affaires dans la recherche et développement. *« Checkmarx n'a guère le profil d'une société de chercheurs : parmi nos employés, on ne compte qu'un Phd (doctorat). Mais l'algorithmique n'est pas seulement fonction des diplômes »*, sourit Emmanuel Benzaquen, lui-même issu d'une école d'application de Polytechnique, titulaire d'un MBA, et qui a sillonné la Silicon Valley. ✖

Nathalie Hamou

> *« Il y a deux ou trois ans, les développeurs ne se préoccupaient guère de sécurité »*
>
> **Emmanuel Benzaquen**
> PDG de Checkmarx

Start-up et PME :

Une solution de surveillance est la clé du succès

Il y a quelques années seules les grandes entreprises surveillaient leurs bandes passantes et la disponibilité de leur réseau informatique. Aujourd'hui presque toutes les PME et les start-ups doivent recourir à un système de surveillance. Or, l'étendue des paramètres à contrôler est plus vaste que jamais, mais avant toute décision d'achat, il est impératif d'identifier ses besoins pour ne pas se perdre dans le nombre des fonctionnalités et des modèles de licences proposés.

Les PME et les start-ups ont un paysage informatique tout aussi complexe que celui des grandes entreprises ; seule l'échelle est différente. Ces entreprises possèdent souvent des équipes informatiques de taille réduite. Aujourd'hui, une infrastructure informatique qui englobe tout le réseau de l'entreprise est absolument indispensable à la réussite de la société. Elle implique l'adoption d'outils annexes, comme PRTG Network Monitor, jouant un rôle croissant dans le succès de l'entreprise. En effet, lorsque des processus cruciaux sont interrompus par des goulots d'étranglement ou autres défaillances, l'impact sur les résultats de l'entreprise est forcément négatif. La surveillance continue des serveurs et des réseaux permet d'identifier et de résoudre les problèmes avant qu'ils ne causent de graves dégâts. Elle contribue à éviter les ralentissements de performance et à améliorer la qualité de service.

Choisir la solution de surveillance réseau idéale

Les PME et les start-ups devraient commencer par déterminer quels domaines sont concernés. PRTG propose diverses options permettant de garder un œil sur l'ensemble du réseau informatique. Pour définir l'ampleur de la solution de surveillance nécessaire, les responsables informatiques doivent commencer par réaliser une analyse en profondeur de tous les éléments essentiels. Il importe de prendre en compte toute future expansion : certains secteurs spécifiques sont-ils destinés à être virtualisés, faut-il prendre en charge la VoIP ou l'IPv6, des filiales devront-elles être incluses dans la surveillance ultérieurement ? Adopter une nouvelle solution ou installer des outils supplémentaires s'avère généralement plus onéreux et demande davantage d'efforts que la mise en place de PRTG dès le départ.

Accompagner l'évolution des besoins

PRTG permet d'éviter l'achat de plusieurs solutions très onéreuses et ne se cantonne pas à la surveillance de la bande passante et de la fluidité du réseau : la solution fournit des données sur les processus du système informatique. Non seulement PRTG surveille le réseau et déclenche une alarme en cas de dysfonctionnement, mais est également soutient activement l'équipe informatique afin de gérer les problèmes dès leur apparition.

Applications pour appareils mobiles

Ces applications permettent de confirmer les alarmes ou de consulter des informations à l'aide de graphiques et de cartes tout en se déplaçant. Les « Tableau de bord » conçus pour les tablettes s'avèrent aussi très pratiques.

Enfin, le prix est un important facteur de décision. PRTG Network Monitor présente des modèles de licences transparents et sans frais cachés. PRTG est facile à configurer et propose des menus clairs.

PRTG est une solution simple d'utilisation et abordable, capable d'assurer la surveillance de l'intégralité du réseau informatique, même à distance.

Saviez-vous que notre licence gratuite de 100 capteurs suffit pour surveiller 20 serveurs et périphériques? Testez par vous-même.

En savoir plus:
www.paessler.com/100capteurs

Pour plus de renseignements sur PRTG Network Monitor, contactez :

Christophe da Fonseca
T : 06 59 77 88 56
info@paessler.com
www.paessler.fr

PAESSLER
the network monitoring company

538027/FR/20150416

Wochit

Le WordPress de la vidéo ?

Ran Oz (gauche) et Dror Ginzberg (droite), cofondateurs de Wochit.

La start-up israélienne Wochit ambitionne de devenir la plate-forme de création vidéo de référence des « story tellers » : et ce, du simple blogueur aux grands médias d'information.

De prime abord, la jeune pousse israélienne Wochit – dont le nom évoque la transcription phonétique de l'expression « Watch it » – a un petit air de déjà vu. Fondée en 2012, la société ne propose-t-elle pas le même service « text to video » que son compatriote Wibbitz, né deux ans plus tôt ? Une start-up qui a fait les gros titres en raison de la notoriété de ses investisseurs : de Kima Ventures, le fonds de Xavier Niel, actionnaire du *Monde*, à Lool Venture et Initial Capital, en passant par le fonds hongkongais Horizons Ventures, sans oublier NantMobile, piloté par le millionnaire Patrick Soon-Shiong qui a encore injecté 8 millions de dollars dans l'affaire en juin dernier.

Et pourtant, les deux sociétés basées entre Tel-Aviv et New-York, et dont l'ambition commune est de révolutionner le story telling, en s'appuyant sur la technologie de traitement du langage naturel (NLP), ne jouent pas vraiment dans la même catégorie. *« Wibbitz se positionne comme une app de news mobile, qui s'adresse au grand public et convertit de façon quasi automatisée du texte en vidéo »*, rappelle Ran Oz, l'un des cofondateurs de Wochit. *« Notre start-up se présente comme une plate-forme de création de vidéos basée sur le Cloud, et proposant des services personnalisées aux grands médias d'information ou au simple blogeur. Nous voulons être le WordPress de la vidéo. »*

Formule gagnante

Rien de moins. Il est vrai que Wochit aligne un tableau de chasse impressionnant avec plus de 300 éditeurs au compteur. En dehors de Reuters et Getty Images – avec lesquels Wibbitz a également noué des partenariats –, la jeune pousse se prévaut de deux accords stratégiques pluriannuels : l'un avec l'agence Associated Press et l'autre, annoncé avant l'été, avec l'Agence France Presse. *« Nous sommes convaincus que Wochit a mis au point une formule gagnante, pour aider les éditeurs, les réseaux ou les indépendants à créer du contenu vidéo digital de qualité à partir de leurs propres articles en quelques minutes »*, a alors fait valoir, Olivier Lombardie, le directeur marketing de l'AFP.

Sur le plan financier, Wochit qui a levé au total près de 15 millions de dollars, peut également se vanter d'un joli tour de table, avec le fonds Cedar, Redpoint Ventures, Greycroft Partners et Marker LLC. Une certitude : la société surfe sur la popularité croissante du format vidéo sur le Web, qui représente déjà 64 % du trafic sur Internet, un chiffre censé grimper à 80 % à l'horizon 2019, selon Cisco. Même si une précision s'impose. *« Notre objectif n'est pas de remplacer un article de presse écrite par un clip vidéo mais d'aider les éditeurs à mettre en valeur leurs articles, avec un complément vidéo de qualité »*, pointe Ran Oz. La preuve : la société israélienne a remporté le prestigieux Prix Gutenberg, pour le saut technologique qu'elle a permis d'effectuer dans le domaine du journalisme. De quoi insuffler un nouvel élan aux géants du print et autres éditeurs en ligne… ✖

NATHALIE HAMOU

Whipclip joue et gagne

Permettre aux consommateurs de créer légalement et de partager leurs propres clips vidéo, réalisés à partir d'émissions de TV ou des contenus de l'industrie musicale. Tel est le créneau imaginé par la firme israélo-américaine Whipclip. La plate-forme mobile a passé des accords avec les principaux réseaux de télévision (ABC, CBS, FOX, etc.) et les grands noms de la musique : Universal Music Group et Sony Music. Le concept séduit. Née voilà seulement un an, Whipclip vient de lever 40 millions de dollars (auprès d'Eminence Capital), et 62 million de dollars depuis sa création. Derrière cette réussite : Richard Rosenblatt et Ori Birnbaum. Ce dernier avait co-fondé Ray V, la plate-forme vidéo en streaming rachetée par Yahoo en juillet 2014.

Déni de service

FAIRE TOMBER UN SITE SOUS LA CHARGE DE TRAVAIL

Les menaces informatiques sont partout : nous en avons sélectionné 6 qui touchent toutes les entreprises. Pour chacune d'elles, nous présentons le principe technique de l'attaque et fournissons de bonnes pratiques pour la contrer. Chaque menace est illustrée avec un cas concret. Comme les attaques par déni de service (DDoS), en deux temps : infection de millions de PC puis attaque coordonnée entre eux vers un serveur. Ainsi le DDoS fait tomber des sites web parfois pendant plusieurs jours.

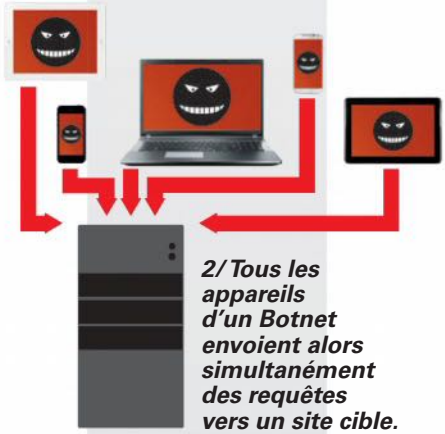
Dossier réalisé par Emilien Ercolani avec Yann Serra

Faire tomber un site web sous le poids des requêtes, tel est le principe de l'attaque par déni de service distribuée – ou DDoS, Distributed Denial of Service attack. *« Le but le plus souvent recherché dans une attaque DDoS est le chantage : on menace une entreprise de rendre inopérants sa boutique en ligne ou ses sites applicatifs si elle ne paie pas une rançon. Et comme une journée chômée coûte très cher en termes de chiffre d'affaires, l'entreprise ciblée préfère généralement payer la rançon »*, explique Laurent Pétroque, responsable avant-vente chez F5 Networks. Selon lui, deux autres motivations existent : on peut faire tomber un site par militantisme politique ou, plus rare, pour affaiblir un concurrent. Dans tous les cas, le site cible est saturé de requêtes, sa mémoire se remplit et son processeur a tellement de données à traiter qu'il n'a plus de temps de calcul suffisant pour exécuter les routines de son système d'exploitation, lequel ne parvient plus à ouvrir de ports pour accepter de nouvelles requêtes. Voire n'a même plus assez de ressources pour assurer la maintenance minimale du serveur. Dès lors, ce dernier finit par planter.

Que le site web visé soit hébergé sur une machine physique ou virtuelle, qu'il soit redondé, qu'il se trouve derrière un pare-feu n'y changent rien : le serveur ne répond plus et il faudra une intervention manuelle pour le faire repartir… Jusqu'à la prochaine saturation. D'ailleurs, les machines virtuelles, si faciles à éteindre et à redémarrer qu'elles

Visualisation d'une attaque DDoS menée par des millions de machines venues de toute part vers une cible unique aux USA.

1/ Un même virus contamine des PC et des smartphones, formant un Botnet et reçoivent un jour un ordre venu d'Internet.



2/ Tous les appareils d'un Botnet envoient alors simultanément des requêtes vers un site cible.

3/ Les requêtes étant tronquées, le serveur du site cible les garde en mémoire où elles s'accumulent ; celle-ci est saturée et le serveur ne répond plus.

4/ Même si la victime parvient à remettre en route le serveur, il continue d'être attaqué durant deux jours.

constituent aujourd'hui l'essentiel des sites web, seraient particulièrement mal loties face à une attaque DDoS. Sans ressource disponible pour que leur OS signale sa détresse à l'hyperviseur, elles seraient compliquées à localiser dans le datacenter et pénaliseraient la puissance de calcul de leurs congénères exécutées sur la même machine physique. Bref, après toutes ces années – la première attaque par déni de service distribuée a eu lieu en 1999 – personne n'a encore trouvé de remède miracle au DDoS.

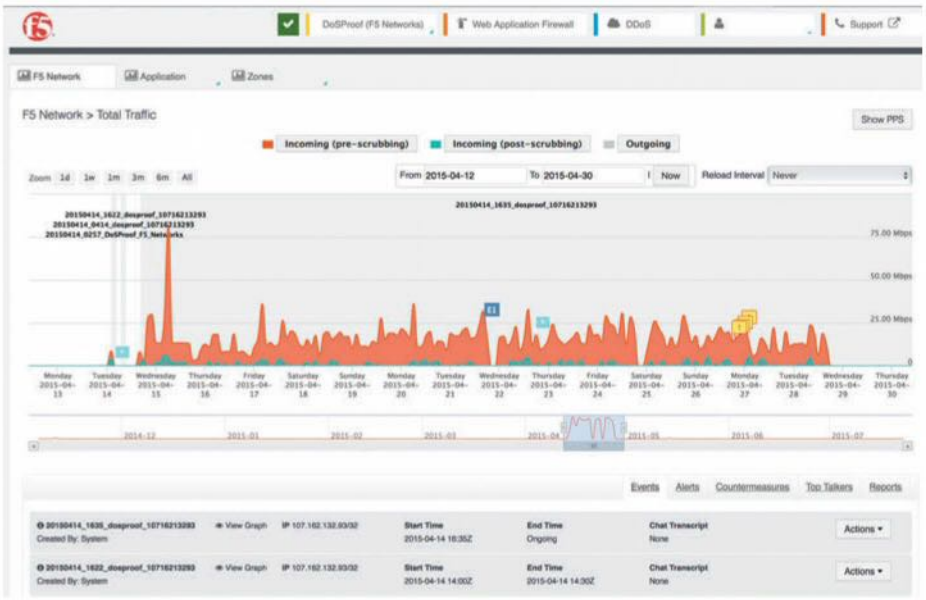
DES ATTAQUES DEPUIS LES SMARTPHONES

De nos jours, les requêtes qui saturent un serveur sont de deux types. Il peut s'agir de requêtes IP bas niveau. *« Ce sont les requêtes d'annuaire DNS ou d'horloge SNTP. Ces protocoles ne demandent aucune authentification, de sorte que tous les serveurs du monde y répondront quel que soit celui qui émet la demande. Il suffit de générer 400 Go de trafic dans ces protocoles pour faire tomber un serveur »*, révèle Laurent Pétroque.
L'autre type d'attaque consiste à envoyer des requêtes applicatives tronquées. *« Dans ce cas, le serveur pense simplement que son client est lent et il laisse la connexion ouverte en attendant la suite du message. L'idée est de le submerger très rapidement de requêtes de ce type, de sorte qu'il n'ait plus aucun port disponible pour accepter des connexions légitimes, ce qui revient à dire que le site web ne répond plus »*, détaille le responsable avant-vente.
Les attaques de DDoS reposent sur l'envoi coordonné de plusieurs milliards de requêtes par jour vers une cible unique. Les expéditeurs de ces requêtes sont des virus qui ont infecté les ordinateurs de monsieur tout le monde et qui attendent patiemment, sans que les utilisateurs ne se doutent de leur présence, qu'un ordre vienne d'Internet pour déverser leurs flots de messages.

CAS CONCRET
Un ultimatum de 48 heures pour payer une rançon

Le cas de la demande de rançon est justement arrivé dernièrement à un site de transaction financière, dont Laurent Pétroque souhaite taire le nom. Depuis décembre 2014, cet organisme était l'objet d'attaques ponctuelles par déni de services. *« Ces attaques parvenaient effectivement à faire tomber leur site momentanément, de quelques minutes à quelques heures. À l'évidence, il devait s'agir d'opérations d'intimidations. Car en mai dernier, quelle ne fut pas la surprise de nos clients de recevoir une demande de rançon. S'ils ne payaient pas, leur site serait 48 heures plus tard indisponible durant deux jours entiers »*, se souvient le responsable avant-vente. Cellule de crise au siège de l'entreprise ! Les dirigeants décident de s'en remettre à la décision de leur département sécurité. Le responsable de cette unité ne compte pas se laisser intimider. *« Pour lui, céder à la terreur reviendrait à laisser la porte ouverte à des demandes de rançon ultérieures »*, raconte Laurent Pétroque. Le montant de la rançon n'a pas été dévoilé.
Dès lors, c'est le branle-bas de combat. F5 Networks propose de filtrer dans son propre datacenter tout le trafic destiné au site de transaction immobilière. L'enjeu : utiliser des switches réseau spéciaux, dotés de puces FPGA spécialement conçues pour reconnaître et éliminer les requêtes tronquées ou celles formatées aux protocoles DNS et SNTP. *« Mais cela ne s'est pas fait simplement. Il a fallu envoyer dare-dare des équipes de F5 Networks chez le client pour reconfigurer tous ses routeurs. Nous avons également demandé à son fournisseur d'accès de modifier les chemins d'accès »*, se souvient Laurent Pétroque. Contre toute attente, les nouveaux raccordements techniques sont opérationnels au bout de 18 heures seulement. Il n'y a dès lors plus qu'à attendre. *« Et, effectivement, à l'heure dite, nous avons vu arriver sur nos routeurs des quantités phénoménales de requêtes tronquées. Elles n'ont pas saturé nos matériels dans le sens où ceux-ci étaient programmés pour les faire disparaître du trafic et non y répondre. Nous avons ainsi pu ne rediriger que des flux sains vers le site de notre client. Celui-ci était d'ailleurs si content de la prestation qu'il a laissé notre solution en place, même au-delà des 48 heures de l'attaque »*, se félicite-t-il. ✖

On parle de PC zombies, amalgamés en un Botnet. Un Botnet est généralement constitué de plusieurs millions de machines infectées. *« L'évolution majeure des attaques de DDoS ces dernières années est que les smartphones, essentiellement des appareils Android, viennent aussi grossir les rangs des Botnets. Les virus les plus répandus pour infecter les machines clientes sont ceux de la famille Dyre. On peut les attraper soit en cliquant sur une pièce attachée frauduleuse dans un e-mail, soit en visitant un site web qui contient un Javascript d'installation »*, relate Laurent Pétroque. Il se refuse à dire que les Mac et les PC Linux sont immunisés : *« Les PC zombies que l'on trouve dans les Botnets tournent pour la plupart sous Windows, certes. Mais c'est essentiellement parce qu'il s'agit de la plate-forme la plus répandue. Techniquement, plus rien n'empêche un virus d'enrôler un Mac ou une machine Linux dans un Botnet »*, avance-t-il.
Autrefois, les PC zombies recevaient leurs ordres de mobilisation sur un port réseau particulier qu'il suffisait de bloquer. Ce n'est plus le cas. Désormais, tous les messages circulent encapsulés dans des paquets HTTP pour tromper la vigilance des pare-feu.



Le déroulement d'une attaque DDoS.

Précisons toutefois que dans le cas particulier d'une demande de rançon, la réussite de l'attaque consiste justement à ce qu'elle n'ait pas lieu. *« Les pirates envoient généralement un ultimatum à leurs victimes 48 heures avant de déclencher l'attaque. Si l'entreprise cible accepte de verser une rançon, son argent est viré sur un compte en banque difficile à investiguer en moins de 48 heures. Ensuite, la somme est éparpillée sur une myriade de comptes en banque et des mules partent le retirer en liquide dans des distributeurs, avec de simples cartes bancaires »*, détaille Laurent Pétroque. ✖

BONNES PRATIQUES
Des contre-mesures qui restent peu efficaces

Les contre-mesures pour parer à une attaque de déni de service distribuée sont multiples, mais aucune n'est à 100% efficace. Les pare-feu permettront de bloquer les attaques IP et, même, toutes celles effectuées sur un port autre que celui dédié au Web. Problème, ils n'arrêtent pas les requêtes applicatives tronquées, ni aucune requête encapsulée dans un paquet HTTP d'ailleurs. Or, toutes les attaques de DDoS modernes autres que IP passent par ce protocole. Quant aux systèmes anti-intrusion IPS, capables d'analyser le contenu de requêtes avant qu'elles n'atteignent les serveurs, ils fonctionnent dès lors qu'ils reconnaissent la signature caractéristique d'un Botnet. *« Le problème est que les Botnets ont entretemps appris à changer tout le temps de signature, y compris entre deux requêtes d'une même attaque »*, avance Laurent Pétroque. De fait, on se tournera plutôt vers des boîtiers réseau de type DDS, qui détectent la répétition exagérée des requêtes de même type et qui, pour l'heure, semblent encore fonctionner. Pour une meilleure efficacité, ce type de boîtiers peut être personnalisé pour reconnaître plus particulièrement un certain type de requêtes, comme dans le cas de la solution de F5 Networks. Le défaut ? Il est probable de que de tels boîtiers éliminent dans la foulée des requêtes légitimes, émises par des clients dont la connexion réseau est véritablement lente. La solution consiste alors à déployer une infrastructure pour mettre sur une ère de garage toutes les requêtes tronquées et à ne les expédier aux serveurs que lorsqu'elles sont complétées. En revanche, cette infrastructure est rarement installable de manière simple dans le datacenter d'une victime, obligeant par conséquent, comme ce fut le cas pour le site de transactions financière à dérouter tout le trafic vers un centre spécialisé.
Dans tous les cas, si une attaque de DDoS survient malgré tout, le premier réflexe doit être de prévenir son fournisseur d'accès pour qu'il route tout le trafic vers un trou noir, épargnant ainsi, au moins, les serveurs. Le résultat, lui, en revanche, reste le même : le site cible est indisponible durant toute l'attaque. ✖

POUR UNE FOIS, PASSER INAPERÇU EST UN AVANTAGE.

Bitdefender innove pour améliorer
la sécurité de vos environnements virtuels
et physiques et économiser vos ressources.
La protection Bitdefender GravityZone est
si légère que vous ne remarquerez même
pas qu'elle est installée.
Ne faites plus aucun compromis
entre légèreté et sécurité.

Testez gratuitement GravityZone :
bitdefender.fr/linformaticien

GravityZone
unfollow the traditional

Bitdefender

Man in the Middle

L'ATTAQUE DE LA TERRE DU MILIEU

Avec le besoin croissant de connexion, tout un chacun cherche à être sur Internet en permanence, quitte à prendre des risques en se connectant n'importe où. Pourtant, cela facilite l'interception d'informations potentiellement sensibles, grâce à des méthodes d'attaques « Man in the Middle » opportunistes ou non.

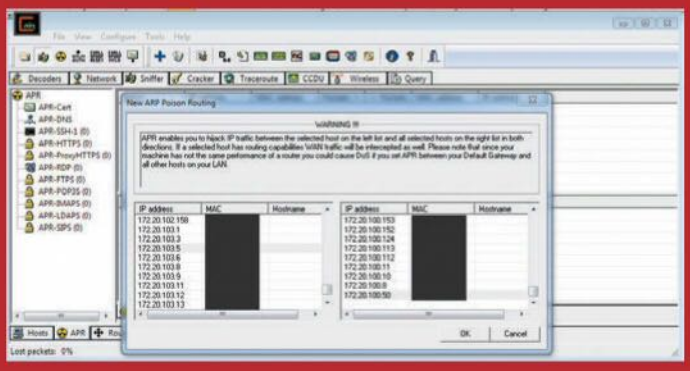
L'attaque « Man in the Middle » (MITM) porte bien son nom : elle consiste à intercepter une information entre deux personnes qui communiquent sur un réseau. Entre A et B, C s'intercale pour récupérer ce qu'il cherche. C'est en théorie aussi simple que cela. En théorie, car dans la pratique cela nécessite tout de même d'avoir le coup de main, ne serait-ce que pour récupérer les clés de chiffrement dans le cadre de l'utilisation d'un VPN par exemple.
On distingue dans les faits trois types d'attaque MITM possible :

1. Interception sur un réseau WiFi ouvert au public.
2. Interception de connexions VPN avec échange de clés de chiffrement.
3. Interception téléphonique.

Dans tous les cas, une personne malintentionnée se glisse dans la communication entre deux points. Il peut s'agir d'un échange direct entre deux ordinateurs ou d'un client vers un serveur par

CAS CONCRET
Le chat et la souris

Les attaques MITM sont complexes et assez sournoises. Et peuvent arriver à toutes les entreprises, peu importe leur niveau de sécurité. Le maillon le plus faible de la chaîne est assis devant son ordinateur : c'est l'humain, le collaborateur. C'est exactement ce qui est arrivé à un gros industriel français. Comme dans de nombreuses entreprises, les cadres sont souvent des experts dans leur domaine mais pas en informatique, et ne sont que trop rarement sensibilisés. C'est d'ailleurs un cadre, en voyage hors de France, qui en a fait les frais. En déplacement à l'étranger donc, la personne a participé à une conférence, un scénario classique qui se répète très souvent. C'est dans un hôtel que s'est déroulé le vol : ses identifiants ont été récupérés par une tierce personne. Tout bêtement, le cadre a voulu se connecter à son espace personnel via un VPN fourni par l'entreprise. Mais en se connectant sur le réseau WiFi de l'hôtel… un type d'installation rarement sécurisé.
L'attaquant a visiblement utilisé un des outils cités dans cet article, ou de même nature. Il a en fait proposé un faux certificat à la victime. Celle-ci s'est

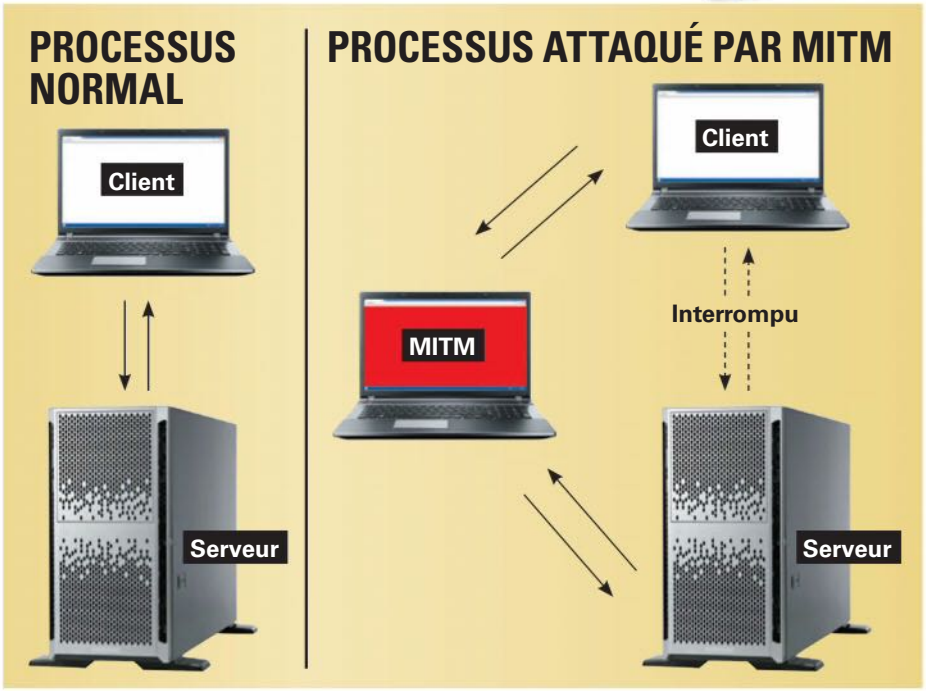


L'outil « Cain » est utilisé pour réaliser des attaques de type MITM par redirection du trafic en « arp poisonning ».

connectée au réseau de l'hôtel puis a lancé sa connexion VPN. Son navigateur l'a pourtant averti en envoyant une alerte *« problème avec le certificat »*. Car tous les navigateurs valident la date d'expiration du certificat et regardent le domaine pour lequel il a été généré. N'y prêtant pas attention, la victime a tout de même choisi de continuer, ignorant ainsi l'alerte. De son côté, l'attaquant a lancé un outil de scan du sous-réseau du WiFi de l'hôtel, pour identifier tous les postes de travail accessibles. Après avoir identifié la passerelle, il injecte de fausses données pour se faire passer pour elle. *« Il n'a pas connaissance à ce moment-là de quelle machine est précisément celle de la victime. Alors, il écoute le*

exemple. L'attaquant joue alors le rôle de relais ou de proxy. Il a pour but de récupérer, en temps réel ou non, des transactions, des conversations ou des données. C'est bien le but de l'attaque MITM : intercepter, envoyer et recevoir des données sans que les intéressés ne soient au courant, en tout cas au moment de l'attaque.

Pour cela, l'attaquant a techniquement besoin d'être sur le même réseau que sa victime. La tâche est bien entendu rendue plus ou moins simple selon le réseau sur lequel est connectée la personne dont il souhaite récupérer les informations. Dans le premier cas, sur un réseau WiFi public, il est possible avec des outils relativement basiques d'intercepter tout le trafic qui transite sur la borne. N'importe qui, connecté sur le réseau WiFi d'un Starbucks ou d'un McDonald, est donc potentiellement une cible. Dans ce cas précis, l'attaquant ne sait pas quelle donnée il recherche exactement : c'est comparable à du « sniffing », c'est-à-dire l'action d'aspirer tout ce qui se trouve alentours. Mais ceci est le scénario le plus simple et peut-être, dirons-nous, le moins efficace en termes de ciblage. Car c'est effectivement un brin plus complexe lorsqu'il s'agit d'attaques plus sophistiquées.



Toutefois, la Toile regorge d'outils très accessibles pour que les attaquants arrivent à leurs fins. Les plus connus sont Ettercap, Cain ou Dsniff. Il s'agit de logiciels qui consistent à s'en prendre aux équipements réseau et à re-router le trafic vers un tiers, en l'occurrence le poste de l'attaquant. C'est aussi ce qu'on appelle du « poisonning ». Dans ce ***trafic WiFi en filtrant sur quelques adresses MAC/IP pour regarder les activités en clair. À partir de là, il fait du profiling »***, **nous explique Vincent Nguyen, responsable technique du CERT de Solucom.**

Ce n'est qu'une fois de retour en France que la victime se rend compte que des fichiers qu'il n'a pas créé apparaissent dans son espace. Il prévient alors le support technique de son entreprise ; l'attaquant avait alors accès au compte du cadre avec ses identifiants. Par chance, un consultant de Solucom était déjà sur place avec les équipes. ***« Nous avons trouvé, après investigations, qu'il y avait des connexions de divers pays depuis l'attaque, en provenance d'Europe de l'Est et des États-Unis notamment. En demandant à la victime ce qu'il s'était passé, elle a donné les informations sur le faux certificat aux équipes internes »***, **précise Vincent Nguyen.**

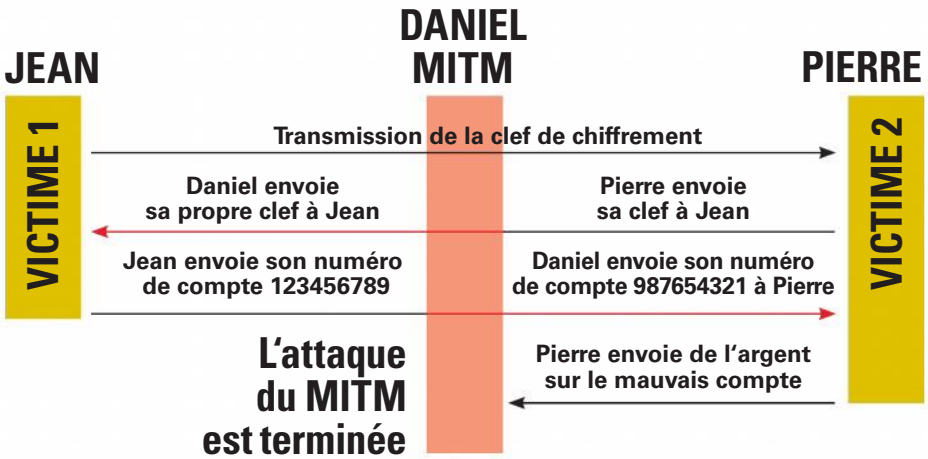
Rapidement, l'entreprise et le CERT de Solucom mettent en place une cellule de crise pour ***« comprendre ce que cherche l'attaquant, ce qu'il a fait, et pour voir si d'autres comptes sont compromis »***. **Trois à cinq personnes sont mobilisées : dans un premier temps, les équipes internes surveillent les connexions alors que celles du CERT cherchent en interne, sur les contrôleurs de domaine.** ***« Nous avons pu détecter quelques applications sur lesquelles l'attaquant s'était connecté, identifier les partages réseau accédés et le type de fichiers recherchés. C'était de la donnée métier très particulière avec des mots clés particuliers. À ce moment-là, nous savions que nous avions à faire à un connaisseur. »***

Pour cela, il faut attendre qu'il se connecte, tracer les connexions et observer son comportement. Le but étant d'avoir une idée la plus complète de ses motivations, des actifs compromis et du périmètre et surtout d'évaluer son niveau de technicité. ***« Il nous faut comprendre si c'est un État ou un étudiant dans sa chambre… ! »***, **s'amuse Vincent Nguyen. En attendant, un plan de défense est établi, alimenté par chaque nouvelle découverte tout en restant silencieux ; l'attaquant ne doit pas savoir qu'il est repéré.** ***« Il y a deux solutions. La première : on est mature pour appliquer le plan de défense et on sort l'attaquant et ferme les vannes tout en l'éjectant du SI. La seconde : on constate que l'attaquant se rapproche d'actifs trop critiques et on déclenche le plan de défense avant de l'avoir achevé. Le but est de fermer à clé la porte principale. Si un seul compte est volé, on renouvelle le mot de passe, voire on crée un nouveau compte et on verrouille l'ancien en re-sécurisant les services. Si nous sommes sur une compromission avancée, et que l'attaquant est devenu administrateur, nous préconisons la reconstruction du domaine. »*** ✖

cas, l'idée est de surcharger les limites techniques des équipements réseau. Il s'agit par exemple d'injecter des fausses données dans les tables desdits équipements en s'appuyant sur de vraies données pour se faire passer pour telle personne ou telle machine. Le problème des équipements réseau les moins bien lotis étant qu'il y existe des limites de nombre d'entrées ; certaines attaques s'appuient sur ces limites pour surcharger les équipements afin qu'ils tombent dans un mode de secours qui va permettre l'attaque. En surcharge, la table se remplie et crée donc des tableaux de données volumineux. Ceci entraîne la suppression de la table et donc les incohérences ne pourront plus être détectées puisque la table est vide.

MITM SUR VPN

Les attaques Man in the Middle peuvent donc être opportunistes – sur un réseau WiFi public – ou plus ciblées – sur un groupe de personnes ou une cible identifiée. C'est très probablement ce qui s'est déroulé dans le cadre de l'attaque contre Gemalto : les experts supposent que la NSA a volé des clés de chiffrement concernant les communications 2G ; une opération clairement destinée à mener des attaques organisées sur des cibles définies. Généralement, les attaques MITM ont pour objet le vol d'identifiants ou de données sensibles. Il existe également un risque de déni de service : pour empêcher la victime de communiquer avec des services externes et que l'attaquant puisse altérer des données. Certaines attaques ont pour but la modification d'informations en temps réel. Là encore, il existe des outils accessibles facilement et capables de reconstruire des flux d'échanges de données, pour reconstituer un tableur Excel par exemple. Il s'agit de Burp ou Web Scarab. Ce sont des proxys applicatifs qui permettent donc d'intercepter des données exploitables et de les modifier. Le MITM a aussi pour but de récupérer des informations même lorsque la victime utilise une connexion sécurisée VPN. L'attaquant « écoute » les réseaux sur un WiFi public – d'un hôtel par exemple –, et, lorsque le collaborateur se connecte, il met en œuvre l'attaque pour détourner les flux, avant que la connexion VPN soit établie. Le principe est de s'appuyer sur le certificat côté serveur (entreprise) et que l'attaquant en présente un faux pour déchiffrer la connexion. Il suffit alors de créer un tunnel chiffré puis, côté infrastructure, monter un autre tunnel chiffré avec le certificat légitime du service. Les navigateurs ont toutefois la capacité d'avertir l'utilisateur lorsqu'ils détectent un problème avec le certificat. L'utilisateur peut aller plus loin s'il le souhaite. Cette fonction est nécessaire car de nombreuses applications d'entreprise possèdent des certificats dits « auto-signés ». Un certificat a, en effet, un certain coût. ✖



PRÉVENTION
Sensibilisation et configuration

« La sensibilisation du personnel et des équipes, ça coûte environ 2 heures et on peut le faire sur plusieurs personnes en même temps. » **Tel est le premier conseil prodigué par le responsable technique du CERT de Solucom. Effectivement, et comme nous l'écrivons plus haut, la faille vient très souvent – trop ? – de l'humain. Mais pas seulement : il existe aussi des cas où les équipements réseau de l'entreprise sont mal configurés. La plupart du temps, les sites des constructeurs fournissent les bonnes pratiques, des guides de configuration efficaces. On peut également trouver ces référentiels sur des sites comme ceux de l'ANSSI ou du NIST (National Institute of Standards and Technology). Attention, toutefois, certains matériels réseau low cost ne possèdent pas ces fonctionnalités de sécurité embarquée. Le choix s'effectue donc également sur les capacités logicielles d'une machine, et pas uniquement matérielles.**

Autre moyen de protection qui tend à se diffuser : le « certificat spinning ». C'est-à-dire que le navigateur client fait lui-même le contrôle du certificat envoyé par le serveur avec un hash en dur dans le code du client. ***« On retrouve ce mécanisme généralement dans les applications développées en interne ou sur celles pour smartphones notamment »*****, souligne Vincent Nguyen. En termes de chiffrement, la nouvelle version de DNSSEC permet d'éviter les attaques de type DNS Poisonning. Plus généralement, il est recommandé de faire appel à des CERT si l'on fait face à ce genre d'attaques. Ils présentent l'avantage d'être pré-contractualisés et donc de pouvoir ouvrir rapidement des tickets d'incident en cas de problème.** ✖

denyall

NE JETEZ PLUS VOS DONNÉES AUX REQUINS !

Les attaques ciblant vos applications sont quotidiennes et létales. Des solutions efficaces existent, et couvrent un océan de risques. Avec DenyAll, préparez votre IT à nager avec les requins.

DenyAll - 6 Avenue de la Cristallerie 92310 Sèvres, France
TEL +33 (0)1 46 20 96 00 - FAX +33 (0)1 46 20 96 02 - WWW.DENYALL.COM

Phishing

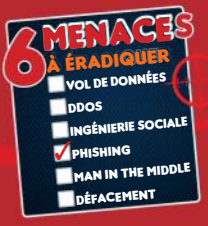
LE PIRATAGE DES COMPTES VIA DES E-MAILS

Le phishing a pour but de capturer le login et le mot de passe d'un internaute avec un mail frauduleux. Qu'importe si ce ne sont pas les identifiants d'un compte en banque, le pirate saura remonter dans la vie privée de sa victime jusqu'à l'un de ses moyens de paiement.

Tout commence par un e-mail de la banque, du fournisseur d'accès, de Google, de Facebook, de PayPal, de l'iTunes Store, ou de n'importe quelle marque qui dispose d'un portail en ligne. Le message invite l'internaute à se connecter, pour consulter un document, valider une opération. Voire, plus urgent, intervenir avant qu'un compte ne soit fermé ou débité. Le lien de connexion est dans le corps de l'e-mail. On clique. Le portail que l'on connaît si bien s'affiche dans le navigateur. On s'authentifie. Mais l'opération échoue, ne mène à rien de concret. Il est déjà trop tard : l'internaute vient de livrer son login et son mot de passe à un malfaiteur qui attendait patiemment de ferrer une victime derrière un site qui n'est pas du tout celui auquel il ressemble.

Le site est parfaitement imité. Et pour cause ! L'attaquant construit sa page avec des liens qui vont chercher les codes HTML et les CSS du site original.

« Après toutes ces années, le phishing est une attaque toujours en expansion car elle permet à coup sûr de gagner de l'argent », lance Sébastien Goutal, le directeur scientifique de Vade Retro. *« Qu'importe le site falsifié. Les internautes utilisant souvent les mêmes Login/mot de passe sur tous leurs comptes en ligne, les identifiants volés sur un faux site DropBox, par exemple, ont toutes les chances de fonctionner sur Facebook ou Google. Or, comme l'authentification sur ces réseaux sociaux sert souvent de clé pour se connecter à toute une*



myriade d'autres comptes en ligne – via le protocole OAuth de délégation d'authentification entre sites web –, le pirate finit toujours par mettre la main sur un moyen de paiement. Ensuite, il s'en sert pour acheter des dizaines d'iPad, qu'il se fait livrer à l'étranger et qu'il revend en France sur LeBonCoin.fr, ce qui lui permet enfin de toucher l'argent de son forfait », ajoute-t-il.

Selon lui, 90 % des attaques de phishing francophones seraient menées depuis la Tunisie et le Maroc. Les 10 % restants auraient pour origine des pays de l'Est, mais aussi le Nigeria. De plus, les gains de l'attaque sont particulièrement rentabilisés : les identifiants peuvent accessoirement servir à accéder à du stockage en ligne de type DropBox pour entreposer les informations dérobées (voire pour les mettre à disposition d'un autre pirate à qui on les aura revendues) et l'argent sert en partie à payer des billets d'avion pour rapatrier en France le matériel acheté en ligne.

UN SITE WEB FALSIFIÉ ET 10 000 E-MAILS INVITANT À S'Y CONNECTER

Dans la pratique, les pirates commencent par louer des serveurs en ligne à l'aide de numéros de carte de crédit précédemment dérobés. Ces serveurs servent à la fois à héberger le faux site et à expédier la campagne d'e-mails qui rabat les internautes vers lui. *« Les Clouds de serveurs en ligne très connus, comme Amazon, ont mis en place des mécanismes qui détectent automatiquement les campagnes de phishing, si bien que les pirates vont plutôt se fournir chez des petits hébergeurs, assez peu regardants quant à l'utilisation de leurs ressources »*, indique Sébastien Goutal. Et de préciser que ces petits hébergeurs ne logent pas forcément en dehors des frontières occidentales. Nombre d'entre eux seraient allemands ou américains. *« Le cas du piratage d'un vrai serveur appartenant à l'entreprise que l'on veut falsifier se présente également de plus en plus. Cela permet d'envoyer des e-mails avec le vrai nom de domaine, afin de tromper les destinataires les plus méfiants »*, remarque Vincent Nguyen, responsable technique du CERT Solucom.

En ce qui concerne la falsification d'un site, Sébastien Goutal note que les pirates parviennent désormais à produire des portails à 99 % identiques à ceux des marques détournées. *« Ils ne cherchent plus à créer des pages HTML*

CAS CONCRET
1,2 million d'euros dérobés à une chaîne hôtelière

Au début de l'année 2015, une campagne de phishing est diffusée de manière plus ou moins aléatoire depuis l'Europe de l'Est. Le contenu de l'e-mail invite à consulter un document sur Google Doc, avec la phrase type : *« Je vous ai envoyé un document, merci de cliquer sur le lien suivant pour le lire. »* Bien évidemment, pour consulter un document Google, il faut soi-même posséder un compte et entrer ses identifiants. Sauf qu'ici le portail n'était qu'une imitation de celui de Google. Vincent Nguyen, responsable technique du CERT Solucom, nous détaille ici toute la procédure imaginée par les pirates : *« Il se trouve que la conciergerie d'un hôtel a cliqué sur le lien, donnant ainsi ses identifiants Google au pirate »*, raconte-t-il. Pour rendre sa campagne de phishing encore plus efficace, l'attaquant s'est alors servi des identifiants de sa victime pour renvoyer l'e-mail frauduleux à tous les contacts de son carnet d'adresse Google.

Les jours passent et ce phishing est à présent répertorié par les filtres anti-phishing des navigateurs web. *« Mais, miracle pour le pirate, le directeur d'un hôtel de la chaîne finit par cliquer à son tour sur le lien. Et il le fait de son iPhone, dont le navigateur n'est pas connecté au filtre anti-phishing des navigateurs sur PC. »*

À ce moment, les attaquants changent de tactique : *« Il est probable qu'ils avaient eux-mêmes disposé des filtres pour identifier des mots-clés comme "directeur" ou "financier". Toujours est-il que le pirate agit à partir de là non plus de l'Europe de l'Est, mais du Nigéria. »*

Durant quatre jours, l'attaquant analyse le compte Google du directeur d'hôtel dont il dispose des identifiants. Parmi les informations qu'il trouve, un formulaire type pour des demandes de virement au siège, ainsi que l'adresse e-mail du responsable financier de la chaîne hôtelière. *« L'attaquant a alors falsifié le document-type en insérant le numéro de l'un de ses comptes bancaires et a formulé une demande de virement de 700 000 €, du siège vers, soi-disant, son hôtel. Il a poussé la contrefaçon jusqu'à imiter les fautes de frappe que le directeur local avait l'habitude de faire dans ses précédents échanges en anglais avec le siège. »*

Quelques jours plus tard, rebelote : il obtient cette fois un virement de 500 000 € de la part du siège. Bien entendu, le formulaire ne suffit pas. Des échanges par e-mail ont lieu à chaque fois pour confirmer l'opération. Mais pour que le véritable directeur local ne s'aperçoive pas des transactions qui se nouent sur son compte, le pirate a l'idée de créer un filtre sur la boîte GMail de sa victime : tous les e-mails envoyés du siège sont automatiquement déplacés dans la corbeille lors de leur réception. L'attaquant parie sur le fait que lui seul aura l'idée d'aller fouiller dedans. *« C'est à la troisième demande de virement que le service financier du siège commence à se poser des questions. Ils appellent alors le directeur local. Lequel nie en bloc les demandes de virement. Mais il est trop tard : 1,2 million d'euros sont partis dans la nature. »* C'est à ce moment que la chaîne hôtelière fait appel à ses services. Il remonte la chaîne de l'attaque jusqu'à l'hameçonnage de la conciergerie, qui a eu lieu 6 mois plus tôt. *« Nous n'avons pas pu leur permettre de récupérer la somme dérobée, mais nous avons pu les conseiller pour que cela n'arrive plus, notamment en ajoutant un dispositif d'authentification forte – avec double identification par login/mot de passe et envoi d'un code par SMS, sachant que l'attaquant n'a pas accès au téléphone de sa victime »*, expliquer Vincent Nguyen en guise de conclusion. ✖

statiques ; ils référencent dans leur code les CSS du véritable site, et présentent des pages qui se mettent à jour en même temps que celles d'origine », explique Sébastien Goutal. Autre preuve du perfectionnement des attaques de phishing, les campagnes d'e-mails sont de plus en plus contextualisées. *« Par exemple, il s'agira d'un e-mail soi-disant envoyé par BNP Paribas pendant Rolland-Garros, ou par les impôts durant la période de déclaration »*, révèle Sébastien Goutal.

La campagne d'envoi d'e-mails dure en général 15 minutes, soit suffisamment peu longtemps pour qu'on ne puisse pas la repérer. *« Contrairement au spam, où il faut envoyer des milliards d'e-mails pour rentabiliser le botnet qui les expédie, une campagne de phishing est rentable avec seulement 10 000 e-mails envoyés »*, dit le directeur scientifique de Vade Retro. Selon lui, sur 10 000 destinataires d'une campagne de phishing, seuls 1 000 comprennent qu'il s'agit d'une escroquerie.

À noter que les pirates programment leur faux site pour qu'il leur envoie par e-mail et le plus vite possible les identifiants capturés. *« Il n'y a pas de bases de données qui stockeraient sur le serveur tous les identifiants en attendant que le pirate vienne chercher sa récolte. Le site frauduleux étant susceptible d'être fermé à tout moment, le pirate s'arrange pour que les informations lui soient remontées en temps réel »*, commente Sébastien Goutal. ✖

BONNES PRATIQUES
La nouvelle tendance tend à enrichir l'attaque avec un malware

Le phishing évolue. Ainsi, depuis le début de l'année, un nouveau type de campagnes provoque le téléchargement supplémentaire d'un malware au moment où l'on clique sur le lien contenu dans l'e-mail frauduleux. Il existe deux types de malware. Le premier, appelé Dridex, va guetter en tâche de fond sur le PC de l'internaute toute opération liée à un compte bancaire, allant jusqu'à prendre une capture d'écran à chaque fois que l'internaute clique sur la page d'un vrai portail. *« Dridex permet typiquement de contourner la saisie d'un code d'authentification par clics successifs sur un pavé numérique dont les chiffres sont disposés dans un ordre aléatoire, ce que font beaucoup les banques, par exemple »*, explique Vincent Nguyen, responsable technique du CERT Solucom.

Le second type de malware est un « ransomware » (logiciel de rançon) : le malware crypte tous les documents présents sur le disque dur de la victime mais aussi sur tous les volumes de données partagés sur son réseau local, puis affiche un message prévenant que les fichiers ne seront récupérables que contre le paiement d'une rançon. *« C'est l'attaque de type phishing la plus populaire depuis janvier dernier. En France, elle a touché des banques et de nombreuses mairies. Pour s'en sortir, il suffit de restaurer une sauvegarde qui date d'avant l'attaque. Le problème est que plus ces sauvegardes sont anciennes, plus le nombre de données perdues est important »*, indique Vincent Nguyen.

ATTENTION AUX NOMS DE DOMAINE

Se prémunir contre le phishing commence par la vérification systématique des fautes d'orthographe dans tous les e-mails qui invitent l'internaute à s'authentifier sur un compte en ligne. *« Désormais, les e-mails de phishing sont majoritairement écrits dans un français correct. Cependant, il reste toujours des fautes, dans le sujet du message notamment, pour passer au travers des filtrages anti-phishing »*, estime Sébastien Goutal, directeur scientifique de Vade Retro. Ensuite, la bonne pratique consiste à toujours vérifier l'adresse de l'expéditeur de l'e-mail. Dans le cas d'un phishing, l'expéditeur a rarement le même nom de domaine que le site officiel qui est censé l'avoir envoyé.

Du côté du navigateur web, tous les logiciels embarquent aujourd'hui une protection anti-phishing qui affiche un message d'alerte lorsque l'internaute clique sur un lien déjà réputé frauduleux. Encore faut-il s'assurer que cette protection est bien activée.

Si la campagne de phishing est suffisamment récente pour ne pas encore avoir été répertoriée, l'internaute doit vérifier l'URL du site sur lequel il arrive. À l'instar du nom de domaine de l'adresse d'expédition de l'e-mail, il est peu probable que cette URL corresponde à l'adresse type du véritable site. Dernière mesure radicale pour éviter de tomber dans le piège du phishing : un véritable portail d'authentification est toujours accédé en HTTPS, alors qu'un portail frauduleux est systématiquement accédé en HTTP. *« Il n'y a quasiment aucun phishing en HTTPS, car les pirates devraient pour cela acheter un certificat, lequel n'est délivré qu'après un contrôle rigoureux »*, assure Sébastien Goutal.

EN CAS D'ATTAQUE RÉUSSIE, PRÉVENIR L'ORGANISME FALSIFIÉ

Et si, quand bien même, *on se fait avoir*, le bon réflexe consiste à prévenir l'organisme dont le portail a été dupliqué. *« Aux États-Unis, la victime d'un phishing sur un compte bancaire perd tout l'argent que le pirate a eu le temps de retirer avec ses identifiants. En France, nous sommes mieux protégés. Si la banque est prévenue, elle couvre la perte. D'autres sites très souvent falsifiés, comme Facebook, sont également très réactifs et bloquent les identifiants volés dans les plus brefs délais »*, témoigne Sébastien Goutal. ✖

1/3

des ordinateurs utilisés de nos jours SONT DÉJÀ INFECTÉS

+72%

d'augmentation des logiciels malveillants ENTRE 2013 ET 2014

UN SIMPLE ANTI-MALWARE NE SUFFIT PLUS.

SECURITE DES EQUIPEMENTS FIXES ET MOBILES

- Windows, Mac et Linux
- Android et iOS
- Sécurité des Serveurs
- Environnements virtuels

ADMINISTRATION CENTRALISÉE

- Security Management (gestion de la sécurité)
- Patch Management (gestion des correctifs)
- Device Management (gestion des appareils)

PROTECTION RESEAU ET CONFIDENTIALITE DES ECHANGES

- VPN mobile sécurisé
- Filtrage des e-mails et sécurité
- Filtrage web

www.f-secure.fr/business

F-Secure.

Ingénierie sociale

LA PORTE D'ENTRÉE EST-ELLE OUVERTE ?

Puisque chacun est un colporteur d'informations potentiellement dangereuses et sensibles pour l'entreprise, l'ingénierie sociale devient de plus en plus cruciale pour les directions informatiques. Web, réseaux sociaux et, bien entendu, téléphone ou phishing : tous les moyens sont bons pour pousser la porte de votre entreprise…

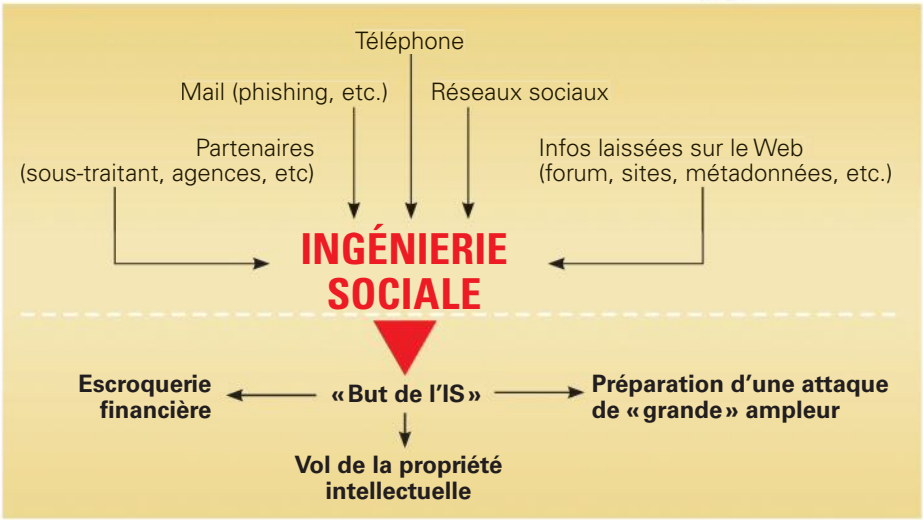
L'ingénierie sociale n'est pas à proprement parler une attaque. C'est un ensemble de menaces protéiformes en perpétuelle évolution, qui grandit avec les nouveaux services qui fleurissent sur le Web, mais également en fonction de ce que font les employés d'une entreprise (vie privée, vie personnelle) ou même de ses partenaires et clients. L'ingénierie sociale est partout, tout le temps. Elle est ubiquitaire et, plus vicieux, prend des formes connues de tous pour mieux leurrer la proie. Le tableau n'est pas joli-joli ! Il y a en fait deux objectifs précis à cela : l'escroquerie et la préparation du terrain. Dans le premier cas, ce seront tous les moyens possibles et imaginables (phishing, escroquerie au téléphone, « fraude au président », usurpation d'identité, etc.) dans le but de dérober soit de l'argent, soit la propriété intellectuelle de l'entreprise. Dans le second cas, il s'agit de tout mettre en œuvre pour lancer une attaque de grande ampleur sur l'entreprise ; un scénario plus probable lorsqu'il concerne de très grandes entreprises voire des gouvernements. Dans ce cas-là, il s'agit surtout de prise d'informations afin de « monter » une autre attaque et ainsi mieux

CAS CONCRET
Audit post-mortem

« *Trouver des informations sur une personne est devenu extrêmement simple sur le Web* », rappelle Yann Le Borgne, directeur technique Europe du Sud chez Cisco. N'importe qui peut créer un faux compte LinkedIn et rapidement commencer par cibler une personne, puis ses contacts et collègues. Et, généralement, c'est ainsi que débute l'histoire : via ces outils totalement intégrés dans nos vies quotidiennes, en apparence inoffensifs. « *Dans la majorité des cas, nous intervenons alors que l'attaque a déjà eu lieu* », précise-t-il, ajoutant que dans le dernier cas grave qu'il a eu à traiter, « *c'était un ensemble de machines qui étaient compromises !* ». En effet, il semble courant que les attaquants ne ciblent pas une personne ou toute l'entreprise, mais plutôt un groupe ou une catégorie de personnes : des cadres dirigeants, le service comptabilité, voire les membres du comité exécutif, par exemple. « *Concrètement, nous commençons par tirer le fil pour voir l'étendue du problème et ses répercussions : généralement, l'attaque vise entre 10 et 15 personnes. Récemment, ce sont des managers qui étaient visés, ciblés avec des mails frauduleux. Nous avons réalisé un audit* « post-mortem ». *C'est-à-dire que nous déployons alors nos outils d'analyse pour comprendre et retracer ce qui s'est exactement passé. C'est ainsi que nous repérons les machines compromises, ce qui permet d'isoler les postes ciblés le plus rapidement possible* », continue-t-il.

La démarche a été suivie par une analyse plus en profondeur sur les différents postes. « *Nous scrutons tout, et notamment la gateway des courriels ainsi que toutes les potentielles zones d'entrée : on recherche l'empreinte partout* », explique encore Yann Le Borgne. D'ailleurs, il est assez rare, voire exceptionnel, qu'une entreprise parvienne à remonter à la source de l'attaque. L'ingénierie sociale peut aussi prendre d'autres formes, comme le « watering hole » qui vise à attaquer une personne par un moyen détourné ; si c'est un développeur, attaquer le forum où il se rend régulièrement par exemple.

la préparer. Globalement, l'ingénierie sociale est en « plein essor » et fait déjà de nombreuses victimes.
Potentiellement, toutes les entreprises sont donc des cibles, car toutes sont exposées. En effet, toutes les entreprises ont des téléphones, des e-mails et une grande majorité une présence sur le Web. Les moyens d'entrer sont donc multiples et variés. Et autant dire que personne ne peut y échapper.
Un exemple assez parlant est celui du spécialiste de la sécurité RSA, victime d'un tel scénario en 2013 : certains employés ayant écrit sur les réseaux sociaux qu'ils cherchaient à partir, des pirates se sont débrouillés pour leur envoyer un tableur Excel leur proposant de la mobilité interne. Bien entendu, les attaquants avaient au préalable récupéré des adresses mails tangibles pour envoyer le leurre. En ouvrant la pièce jointe, la porte de l'entreprise venait de s'ouvrir…
Autre cas, plus récent. C'est ce qu'on appelle « l'escroquerie au président ». Il s'agit du cas d'une aide comptable d'une mutuelle de Nancy. Coup sur coup, le – faux – président de son groupe et un avocat – un certain Maître Lacombe – lui ont demandé de virer 252 000 euros sur un compte dans le cadre de la préparation d'une fusion. La malheureuse aide-comptable était non-habilitée pour exécuter ce genre d'opération. Mais les deux escrocs ont insisté sur le caractère confidentiel de l'opération. Ils ont joué sur l'affect, la confidence et la confiance. Résultat : la somme s'est envolée dans la nature, et l'aide-comptable est accusée de « complicité implicite du délit d'évasion fiscale et de blanchiment d'argent ». Le nombre de ces cas est difficile à recenser précisément, car les entreprises ne s'en vantent pas. Selon une source syndicale, plus de 350 entreprises françaises ont été victimes d'un tel scénario d'ingénierie sociale en 2013. ✖



BONNES PRATIQUES

Il y a bien entendu des méthodes simples pour commencer à se protéger face à ce genre d'attaques. La première d'entre elles est peut-être simplement d'édicter des règles et rappeler les basiques. Outre la protection contre le phishing – évoquée dans notre dossier –, il y a les bons réflexes : à commencer par se méfier de tout ce qui vient de l'extérieur. *« Si quelqu'un appelle d'un poste en dehors de l'entreprise, demander à ce que la personne rappelle de l'interne »*, souligne Yann Le Borgne. Mais il y a aussi une solution dite d'éducation, qui peut passer par des éléments très basiques. On pense notamment à rappeler aux employés qu'il existe une distinction entre vie professionnelle et vie privée. Et cela s'étend même au CV que l'on peut mettre en ligne par exemple ; des compétences très explicites peuvent attirer l'attention et être le point d'ancrage pour amorcer une attaque en vue d'un vol de propriété intellectuelle.
Mais les employés ne sont pas les seuls à devoir être éduqués. L'entreprise toute entière doit prendre conscience de ce qu'elle publie. Par exemple, nous pensons aux métadonnées des documents diffusés qui, utilisées à grande échelle, peuvent donner une cartographie de l'entreprise et de ses process. Une source d'information très intéressante pour quelqu'un de malintentionné. Certains ont d'ailleurs mis en place des outils de protection contre la récupération des métadonnées. Enfin, la population ironiquement la plus sensible à ces pratiques est celle de l'informatique, qui transgresse souvent ses propres règles. C'est l'histoire du cordonnier mal chaussé… *« Je me souviens d'un RSSI qui avait fait des campagnes de phishing pour sensibiliser les gens. Par ce moyen insolite d'éducation, il avait réussi à faire passer concrètement un message. Tout le monde y était sensible, sauf les gens de l'IT ! »*, poursuit Yann Le Borgne. En effet, ces derniers, bien que curieux et ayant repéré la supercherie, cherchaient effectivement à savoir d'où venait l'attaque et comprendre son fonctionnement ; *« Voilà pourquoi ils tombaient, volontairement, toujours dans le panneau ! »*
Pour éduquer les gens, certaines entreprises ont mis en place des campagnes répressives. À l'inverse, d'autres ont testé des méthodes éducatives, avec des lots à gagner pour mieux sensibiliser les plus attentifs et réceptifs aux messages. Impliquer les gens : et cela fonctionne, semble-t-il…
Mais dans un monde où il n'est désormais plus possible de se prémunir de toutes les formes d'attaques, il faut changer de paradigme. Il ne s'agit pas de remettre en cause le travail en matière de sécurité informatique des dernières années. En revanche, il faut se préparer à savoir et pouvoir réagir vite et bien : garder des traces, former les gens et concevoir de véritables process « de crise ». *« Je peux assurer que si quelqu'un veut rentrer dans votre entreprise, peu importe comment il y arrivera. Il y a toujours un point faible »*, conclut Yann Le Borgne. ✖

Défacement

GARDER SON SITE INVIOLÉ

Le « défacement » consiste principalement à changer la page d'accueil d'un site. Et les moyens d'y parvenir sont nombreux. Heureusement, il existe des solutions pour éviter le problème, ou tout du moins pour limiter les possibilités.

Imaginez que vous vous rendez sur votre site. Et là apparaît un message qui n'a rien à voir avec ce que vous attendiez, une revendication, sur la page d'accueil. Vous venez d'être « défacé ». Dans la plupart des cas, le défacement de site web n'a qu'un objectif, souvent politique : faire passer un message. Et autant dire que les sites ne sont pas visés au hasard.

Tous les sites ne sont pas égaux devant cette menace ; à partir du moment où ils sont maintenus et à jour, CMS y compris. La plus grande différence se situe entre sites statiques et dynamiques. Pour les premiers, il est relativement simple de se prémunir contre une attaque de défacement (cf. la rubrique Prévention). Pour les seconds, il faut se méfier du code applicatif, porte d'entrée pour les injections notamment.

Une telle attaque arrive le plus souvent via trois techniques :

- l'exploitation d'une faille dans le CMS ;
- l'ingénierie sociale – dans le cas où l'attaquant modifie les mots de passe et l'enregistrement DNS pour faire pointer vers un autre site ;
- le Spear Phishing, qui cible une population précise dans l'entreprise pour récupérer des identifiants/mots de passe.

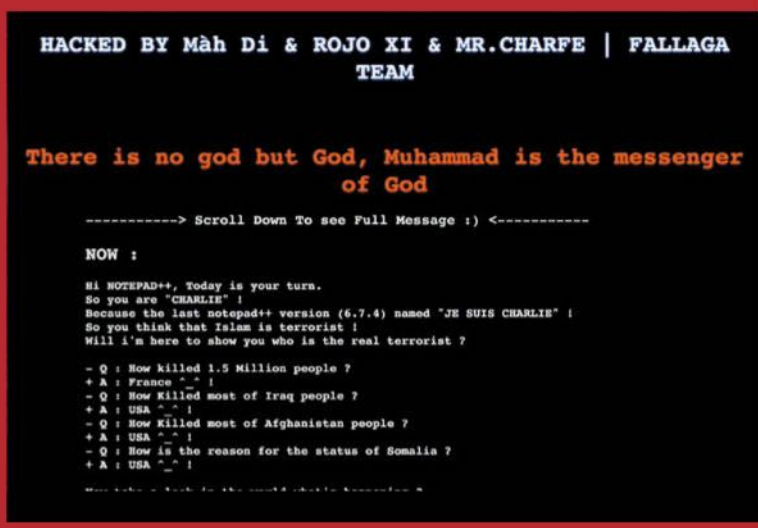
Dans tous les cas, il s'agit bien de récupérer des accès pour modifier le fichier index.htm du site. Il existe d'ailleurs plusieurs « niveaux » de défacement. Celui où l'attaquant modifie simplement le fichier index.htm pour faire apparaître un message sur la page d'accueil. Dans ce cas, il « suffit » de reprendre une sauvegarde et de replacer le bon index.htm. Puis un autre cas où l'attaquant est entré en profondeur dans le système, et peut tout mettre en place pour vous gâcher la vie. Par exemple, il peut créer une page pour automatiser le redéploiement de sa propre page.

De plus, le défacement peut faire beaucoup plus mal ; c'est une « tendance » de 2015 ! La technique s'inspire du ransomware, dans lequel un attaquant vole des données sur une machine et demande une rançon pour les redonner. En fait, elle utilise le même principe mais sur un site web. *« Si un attaquant vise par exemple un site d'e-commerce avec une base de données derrière l'application, il va modifier les scripts pour introduire une notion de chiffrement. Progressivement, il chiffre la base de données mais également les backups »*, explique Luis Delabarre, chez Hexis Cyber Solutions. Imaginez la rançon demandée pour récupérer la base de données d'un site d'e-commerce…

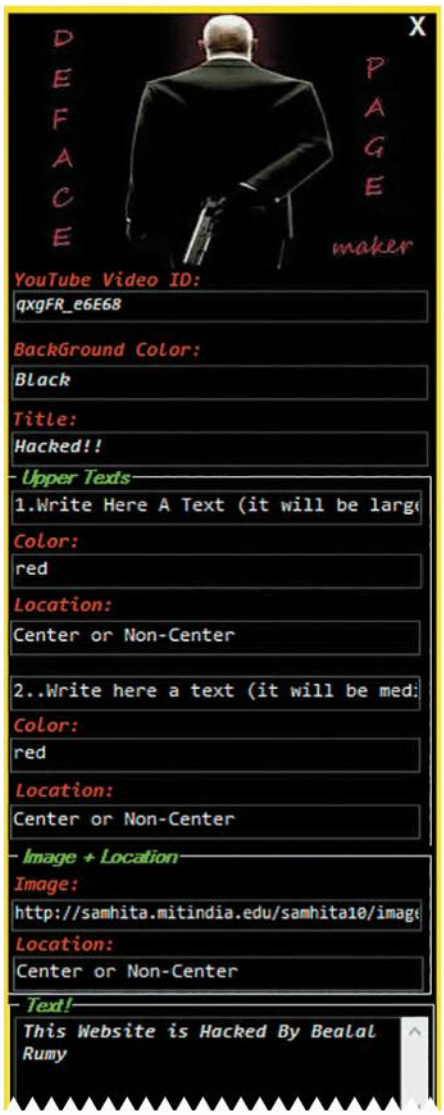
CAS CONCRET
Le défacement, c'est pas Charlie

Il existe de très nombreux exemples de défacement de sites web. Dans certains cas, le défacement est réalisé simplement pour l'honneur. Le site du MIT en avait fait les frais, avec sa page d'accueil modifiée pour « célébrer » la mort de l'activiste Aaron Swartz. Plus récemment, le constructeur Tesla avait été attaqué, tout comme Lenovo avec du DNS Hijack par le groupe de pirates Lizard Squad.

Mais, en début d'année, une vague d'attaque de défacements sans précédent a touché des milliers de sites français. Suite aux tragiques événements de Charlie

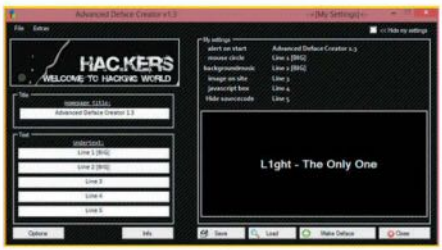


En janvier 2015, le site de l'éditeur HTML Notepad++ avait été défacé par la « Fallaga Team »



DÉTECTER UN DÉFACEMENT

Ce ne sont pas des méthodes de prévention mais plutôt une surveillance qui devrait être effectuée régulièrement. Car il est possible de détecter les signaux d'une tentative de défacement, sans recourir à rien de très technique. Tout d'abord en regardant régulièrement le poids de la page web. Car un défacement peut aussi se contenter de changer uniquement quelques éléments de la page. Si l'attaque est sur le point d'intervenir, c'est que l'attaquant va remplacer tout le contenu par le sien : une image en général. Ainsi, le poids sera considérablement réduit. Autre conseil : prendre régulièrement des copies d'écran du site et les comparer. Enfin, vous pouvez aussi en vous connectant au site rechercher une chaîne de caractères représentative de votre site. Il est fortement conseillé d'utiliser un service de supervision en ligne. Certains de ces services peuvent par exemple vous alerter si la chaîne de caractères que vous avez indiquée change. Essayez le très bon https://checkmy.ws/fr/. ✖



Deux outils utilisés pour créer des pages types de défacement.

Hebdo, les Anonymous avaient attaqué des sites islamistes, en représailles. Mais la contre-attaque a eu lieu : c'est l'« Opération France ». Des centaines de sites d'entreprises, médias, ministères et autres, représentants les intérêts de la France, ont été ciblés. Le CERT français a été mis en alerte. *« Nous nous attendions à de grosses attaques mais il n'y en a pas eu. Il y en a eu de très nombreuses mais d'une complexité faible »*, nous explique un expert qui a participé à la défense des sites français. Dans cette vague d'attaques, les pirates ont très probablement simplement regardé les domaines enregistrés en France et les ont attaqué ; ce qui explique l'ampleur. En revanche, l'attaque était automatisée notamment avec des exploits de CMS (WordPress, Joomla, Drupal, etc.). *« Une entreprise que nous suivons a vu ses cinq sites défacés. Immédiatement, nous avons cherché à voir si l'attaquant était allé plus loin dans le SI. Il s'est avéré que non »*, explique l'expert qui ajoute que c'est *la* question qu'il faut se poser après avoir été attaqué. Tous les sites du client avaient un point commun : ils n'étaient pas à jour ! Résultat, toutes les pages d'accueil changées avec des messages à caractère politico-religieux. *« Dans ce cas-là, il faut commencer par mettre à jour le CMS pour combler les failles. Ensuite, récupérer la sauvegarde et rétablir les fichiers changés. En général, le retour à une situation normale est assez simple et rapide »*, poursuit-il. ✖

BONNES PRATIQUES

Il existe tout d'abord des outils en ligne de monitoring de vos sites web. Le plus simplement possible, il convient tout d'abord de sécuriser au maximum le CMS en lui-même. Il existe d'ailleurs de nombreux plug-ins qui peuvent commencer à renforcer la sécurité de votre site web à l'instar d'Anti CRSF pour WordPress, qui vérifie les permissions d'une installation WordPress.
Mais la première des protections commence au moment où vous enregistrez un nom de domaine : ne mettez jamais de coordonnées de personnes physiques – elles peuvent aider à l'identification et donc le ciblage de l'administrateur. De plus, pensez de suite à changer le mot de passe pour un autre beaucoup plus solide. Autre conseil logique : se renseigner sur le versioning du CMS choisi, la fréquence des mises à jour et le moyen d'installation, surtout dans le cas où vous devez gérer du multi-site. Regardez également ce que font les hébergeurs, dont les offres évoluent rapidement en matière de sécurité. Microsoft propose désormais avec Azure une option par défaut Mode Security, un WAF. Au-delà du choix d'un hébergeur, un autre maillon peut être critique : l'agence web, qui gère souvent la partie applicative, et qui choisit elle-même l'hébergeur.
Ce sont de bonnes pratiques qui sont d'un niveau basique. Outre cela, et suivant le niveau de protection souhaité, les administrateurs peuvent mettre en œuvre des outils et stratégies de détection des attaques plus avancés ; notamment dans le cas où un site est une cible régulière. Mais ce qui fait souvent défaut au quotidien, c'est la gestion du déploiement des patchs (patch management), essentielle lorsqu'un administrateur gère plusieurs plates-formes. Là encore, en termes de protection, l'Anssi donne des conseils en matière de protection. ✖

Vol de données

LA GOUVERNANCE À LA RESCOUSSE ?

Par manque de temps ou d'argent, ou par volonté de ne pas précipiter ou retarder des chantiers primordiaux, de plus en plus d'entreprises sont victimes de vols de données au sein de leur base de données. Comment repenser l'organisation pour assurer la sécurité des données de l'entreprise ? La gouvernance et une sérieuse remise en question de l'architecture peuvent être les premières réponses.

Ces dernières années, il n'a pas été rare de constater dans l'actualité des entreprises dont les données ont été volées. Les cas se multiplient ces derniers temps : les bases de données se font dérober par des pirates, parfoit pour le prestige, des données importantes voire vitales à l'entreprise car touchant son cœur de métier. L'un des derniers cas emblématiques est celui de Domino's Pizza, qui s'est fait dérober pas moins de 650 000 données clients. Plus récemment, le site Labio.fr, d'un laboratoire de biologie médicale du sud de la France, qui s'est fait voler 40 000 données de ses patients. Les pirates de Rex Mundi ont demandé une rançon. Ces derniers écrivaient que les sites qu'ils attaquent *« ont tous un point commun : des protocoles de sécurité médiocres ou des applications web mal conçues »*.

C'est là où le bât blesse, car même dans le cas où les données de l'entreprise sont primordiales, la sécurité est délaissée. Et le parent pauvre du SI, assurent de nombreux experts, puisqu'elle passe après l'achat de matériels, de formations, etc. Le problème étant que l'IT dans les entreprises évolue en permanence, alors que les services de sécurité ont du mal à s'adapter à ces changements. Plus grave : ce ne sont pas toujours les personnes en charge de la sécurité qui s'occupent des bases de données au jour le jour. Enfin, la multiplication des services, des offres déportées (SaaS/Cloud), etc., crée autant de portes d'entrées pour pénétrer dans le SI d'une organisation. Sans oublier le fameux « shadow IT », par le biais duquel les différentes divisions de l'entreprise choisissent et souscrivent elles-mêmes à des services en ligne, sans

CAS CONCRET
Attaque progressive

Comme toujours, lorsqu'on parle de sécurité informatique, aucune entreprise n'est à l'abri. Et nous le vérifions encore une fois en ce qui concerne le vol de données : dans le cas que nous vous relatons ici, c'est une entreprise du CAC 40 qui en a été la victime. Et comme souvent, l'attaque débute en cherchant à récolter des informations pour prendre la main à distance. Le problème dans ce cas est l'organisation de la DSI : si l'entreprise possède une IT centrale, elle dispose également de délégations dans de nombreux pays, créant des conflits Paris/province ou France/reste-du-monde. La complexité de l'architecture peut rendre plus simple la tâche des attaquants ; chacun se renvoyant souvent la balle sur les responsabilités. Ce qu'il s'est passé : l'attaquant a donc cherché à entrer dans le SI en utilisant du phishing. L'opération est assez classique dans le sens où il a envoyé un mail contenant un ver à une personne de la logistique. Vide, l'opérateur continue comme si de rien n'était, sans s'apercevoir qu'il venait de se faire hameçonner.

À partir de là, l'attaquant peut faire de la prise en main à distance via une connexion chiffrée ; les proxys sont alors aveugles. Mais l'attaque a été réalisée de manière progressive : le poste était contaminé mais le pirate a attendu, patiemment. *« Les responsables de l'IT ont eu un coup de chance »*, sourit Arnaud Cassagne, chez Nomios, qui a participé à la résolution de cette affaire. *« Sans indicateurs particuliers, ils ont décidé de lancer un audit pour évaluer leur niveau de sécurité. Ils pensaient trouver des machines corrompues, et c'était le cas »*. Débute alors une phase d'échanges et d'entretiens avec plusieurs personnes de l'entreprise dans le but de

passer par la DSI. Phishing, ingénierie sociale, malwares… Toutes ces techniques ont pour but de mettre la main sur un compte à privilèges qui permettra d'accéder à des données et donc de les extraire hors des murs de l'entreprise. Car la plupart du temps, c'est un fait, les entreprises partagent un compte à privilège entre plusieurs administrateurs : une erreur fréquente qui facilite amplement le « travail » d'un potentiel attaquant.
L'erreur de base est de considérer que les bases de données sont un actif comme les autres : c'est une affaire de spécialistes, tant au niveau de la gestion que de la programmation. De plus, certains experts affirment que jusqu'à 80 % des serveurs de base de données ne sont jamais mis à jour, et restent avec leur SGBD initial. Ce qui a donc pour conséquence de laisser des brèches béantes qui ne sont jamais corrigées, et notamment sur les réseaux internes. Mais comme nous le voyons avec les différentes attaques de ce dossier, si pénétrer le système d'information d'une entreprise n'est pas facile, l'opération est tout de même largement faisable. Enfin, la criticité de certaines applications empêche les arrêts pour maintenance : la sécurité passe encore en dernier… La plupart des bases de données sont aussi installées via un logiciel tiers (un ERP, etc.) et restent installées « par défaut », sans configuration. Ces mauvaises configurations conservent souvent un mot de passe par défaut (dans 80 % des cas !) ou des modes d'authentification dégradés (.rhosts ou OPS$). Ces différents éléments laissent donc la porte ouverte à de nombreux types d'attaques, sur les applicatifs (injections SQL, détournement des requêtes, autorisations trop larges) ou sur l'OS via le SGBD notamment (écriture/lecture de fichiers, exécution de commandes, contournement de la politique de sécurité, "safe_mode" de PHP, etc.). ✖

Un des outils Imperva utilisés pour résoudre le vol dans la base de données de cet exemple.

« comprendre leur métier, déceler les points forts, faiblesses, les briques en place, versions des applicatifs, niveau d'utilisation… Bref, de voir le niveau de maturité ». Avec du renfort, Nomios a travaillé avec ses propres outils : firewall, cartographie, solutions anti APT (Advanced Persistent Threat), analyse comportementales pour voir si des choses curieuses qui transitent sur le réseau. Mais aussi : enregistrement des flux du sur le réseau qui sont des *« traces réelles où l'on extrait des fichiers, des menaces, des conversations ou des mails »*. Une solution de gestion des logs est également mise en place. *« Nous corrélons toutes les alertes pour comprendre ce qui est vraiment malveillant, en une ou deux journées. La configuration c'est facile ; c'est l'analyse qui prend du temps… »*, souligne Arnaud Cassagne.
La base de données est donc passée au peigne fin, avec un outil d'analyse permettant de surveiller si un compte récupère plus d'éléments qu'en temps normal, et cherche des fichiers sensibles. *« Dans ce cas précis, le malware s'était propagé sur plusieurs machines, jusqu'à celle d'un administrateur »*. Un canal de communication chiffré sortait des centaines de Gigaoctets, du document basique aux process industriels. En approfondissant, les accès ont donc été restreints et la communication coupée après avoir été identifiée, puis l'attaquant jeté hors du système. ✖

6 MENACES À ÉRADIQUER
- ☑ VOL DE DONNÉES
- ☐ DDOS
- ☐ INGÉNIERIE SOCIALE
- ☐ PHISHING
- ☐ MAN IN THE MIDDLE
- ☐ DÉFACEMENT

BONNES PRATIQUES

Comme illustré dans le cas concret, la gestion des systèmes est de plus en plus complexe dans de nombreuses entreprises. Ici, c'est le manque d'utilisation approfondie des outils en place qui a fait défaut. Il faut prendre du temps pour analyser ! De plus, *« tout le monde a désormais de nombreux onglets ouverts en permanence. Il devient très complexe de savoir qui est un potentiel attaquant »*, explique Arnaud Cassagne, soulignant que le niveau de détails a beaucoup augmenté ces dernières années.
Il existe bien entendu des réponses aux vols de données. Une tendance actuelle, en provenance des gros acteurs du Web, est la DevSecOps ; dérivée de la DevOps, appliquée à la sécurité. Il s'agit de créer de petites équipes dynamiques et multicompétentes avec un objectif commun. *« Ensemble, elles montent une plate-forme et travaillent de concert »*, précise le spécialiste de Nomios. Au-delà de cette tendance, il est d'usage de travailler un process en 5 étapes, à commencer par un audit pour savoir qui accède à quoi, quand et comment sur la base de données. En second lieu, opter pour un firewall en dérivation sur la base de données si ce n'est pas le cas. En troisième, concevoir un plan de réponse en cas d'incident. *« Il faut imaginer les pires des scénarios. Et pour cela, le mieux est de se renseigner, communiquer avec les confrères, etc. »* Le plan doit également intégrer les bons contacts en cas de problème très grave. En quatrième position, appliquer des règles sur un petit périmètre, puis au fur et à mesure sur tout le périmètre de l'entreprise. Enfin, *« remettre en cause ses choix »*. Tout cela s'insère dans un processus de gouvernance qui devient primordial dans de plus en plus d'entreprises et qui se traduit par la règle des « 3P » pour « People, products, process ».

REPORTAGE

Cybersécurité

Les experts de Trend Micro en action

Le centre de recherche en cybersécurité de Trend Micro, implanté aux Philippines, est une ruche où plus de 1 000 employés traquent jour et nuit les virus et autres attaques menées contre les systèmes d'information de leurs clients. Le centre dispense sa propre formation et possède même son « équipe d'enquêteurs ». Reportage chez des experts de la sécurité numérique.

L'ambiance est studieuse. Curieusement, pas aussi bruyante que l'on s'y attend en entrant dans ce vaste open space rempli de box où des dizaines d'employés sont penchés sur leurs écrans, beaucoup d'entre eux portent un T-shirt rouge marqué du logo de l'entreprise. Ce qui se joue ici est d'importance. Nous sommes au cœur des TrendLabs, le laboratoire de recherche en cybersécurité de Trend Micro. Pas moins de 1 200 personnes traquent les attaques, virus et autres malwares 24 heures sur 24 et 7 jours sur 7. Seul centre de cybersécurité aux Philippines, les TrendLabs sont aussi le plus important centre de ce type dans toute la zone Asie-Pacifique.

Des jeunes, des femmes, un bon système éducatif

Ce qui frappe quand on entre dans ces locaux, très protégés, est la jeunesse des employés. Près de 3 sur 5 (59 %) ont entre 20 et 29 ans. Les jeunes femmes sont nettement plus présentes que dans une société occidentale, 40% des employés des TrendLabs sont en effet des femmes.

C'est au cœur de Manille, capitale des Philippines, que Trend Micro a installé son centre de cybersécurité. Pourquoi avoir choisi les Philippines ? *« Après avoir été colonisées par les Espagnols, les Philippines ont été colonisées par les Américains. Notre système d'éducation est très américanisé et tous les Philippins parlent anglais. De plus, ce système d'éducation fournit 300 000 ingénieurs en informatique chaque année ! Outre que cela coûte moins cher de faire du business en Asie, nous sommes proches du siège de l'entreprise, qui est au Japon, à Tokyo »*, explique Myla Pilao, directeur du marketing des TrendLabs. Ajoutons à cela que les Philippines ont – relativement – échappé à la crise économique de 2008 et que, suite aux révélations d'Edward Snowden, le fait de ne pas être une société américaine est plutôt un atout dans le monde de la cybersécurité. Myla Pilao ajoute : *« Ici, nous avons trois points forts : la nourriture, le sport – notamment la boxe – et la sécurité ! »* Ce n'est pas un vain mot. Et il ne s'agit pas seulement de sécurité logique ! À chaque coin de rue de Manille, devant chaque banque, immeuble de bureaux, résidence ou hôtel, des gardes armés veillent.

Trend Micro

La société a été créée en 1988 à Los Angeles (Californie) par Steve et Jenny Chang et Eva Chen. Cette dernière dirige la société depuis 2005. En 1992, le siège est déplacé au Japon et la société entre en Bourse à Tokyo en 1998.
Aujourd'hui, Trend Micro emploie 5 200 personnes sur 38 sites dans le monde. Elle compte plus de 500 000 clients dont 48 des 50 premières entreprises mondiales. En 2014, elle a réalisé un chiffre d'affaires de 1,1 milliard de dollars américains.

Et personne ne s'en offusque. La sécurité fait partie du quotidien des Philippins. C'est donc tout naturellement que les jeunes – et pas seulement les ingénieurs – rejoignent les rangs des TrendLabs.

Enseigner l'assembleur

Pour les recruter et s'assurer de leurs compétences, la société a mis au point son propre programme de formation, la Trend University. Les jeunes diplômés y suivent 5 à 6 mois de cours intensifs pendant lesquels ils sont rémunérés. *« Nous leur enseignons surtout l'assembleur, c'est le langage le plus important pour notre activité et il n'est pas ou peu enseigné aujourd'hui »*, explique Nicholas, en charge de la Trend University. Pour obtenir leur qualification, les candidats doivent réussir un examen. Puis ils partent passer un mois dans un centre Trend Micro à l'étranger. *« La formation est intense et elle ne porte pas seulement sur le savoir-faire et les compétences techniques. Les candidats doivent aussi montrer leurs capacités à travailler en équipe et un savoir-être au travail »*, poursuit Nicholas. Chaque session de formation compte entre 10 et 12 personnes. Les TrendLabs en organisent trois par an.

L'histoire raconte que l'un des créateurs philippins du ver informatique *I Love You*, alias *Love Letter*, ver qui a causé plusieurs milliards de dollars de dégâts en l'an 2000, a été candidat à un emploi aux TrendLabs. Sans succès! *« Nous ne franchissons pas la ligne »*, résume Myla Pilao, *« Nous ne recrutons pas dans le dark web. Et nous menons de nombreux entretiens avec les candidats pour nous assurer de leur bonne foi. »* Moyennant quoi, les employés des TrendLabs démarrent avec un salaire de 600 à 700 euros, soit trois fois plus que le salaire moyen aux Philippines, d'environ 200 euros.

Des millions de spams bloqués chaque jour

Les services sont organisés par type et par niveau de réponse. Le service « email reputation » bloque les spams et inspecte les mails douteux afin d'établir la blacklist et enrichir la base de données « empreintes » des mails frauduleux. Chaque jour, l'équipe de 25 personnes bloque entre 2 et 4 millions de spams. De 3000 à 5 000 e-mails sont inspectés manuellement. Le service « web reputation » détectent les sites qui émettent malwares, phishing et autres attaques. Pour assurer un service continu, l'ensemble de l'équipe travaillent 13 heures par jour, un jour sur deux. Le service estime à 5 millions le nombre d'URL bloquées chaque jour. Le service « file reputation » analyse les fichiers et les pièces jointes. Les 150 personnes de l'équipe sont réparties entre les États-Unis et les Philippines. Chaque pays assure le service pendant 12 heures. Quelque 40000 cas sont gérés par mois.

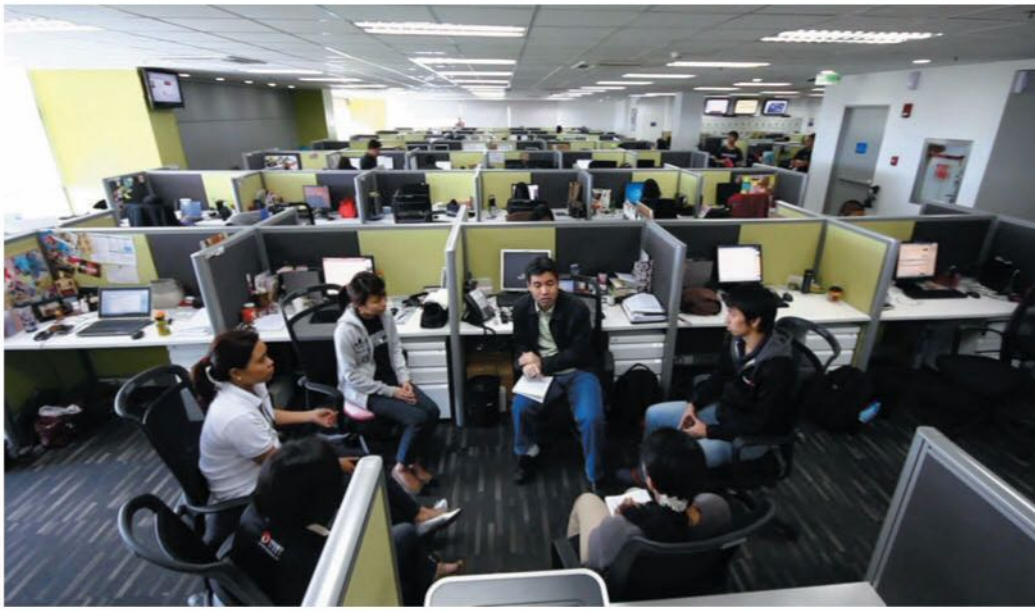
Pour déceler et tester les malwares, les employés utilisent des machines virtuelles (VMware) sous Linux, des logiciels open source et de nombreux outils logiciels maison sur lesquels Trend Micro préfère rester discret…

Enfin, l'équipe « Advanced Threat Research » mène des enquêtes prospectives. Cette équipe n'a pas de rôle opérationnel. *« Nous menons des enquêtes, parfois longues, souvent en relation avec les forces de l'ordre ou Interpol, puis nous publions nos résultats »*, explique Ryan Flores, directeur de l'équipe. Composé de 21 personnes, ce groupe affiche une moyenne d'âge de 35 ans, supérieure à celle des autres services, *« le plus âgé de l'équipe a 50 ans »*, précise Ryan Flores! Il énumère les succès du groupe, les Estoniens de Ghost Click, la fraude porno asiatique Sextortion, le pirate algérien arrêté en Thaïlande, etc. Le problème est que les pirates sont aujourd'hui aussi bien formés et aussi organisés que les employés des entreprises de sécurité! Même dans le monde numérique qui est le nôtre, les méchants garderaient une longueur d'avance sur les gentils! ✖

SOPHY CAULIER

Des menaces en constante évolution

« La cybersécurité fait désormais partie des préoccupations majeures des dirigeants », reconnaît Myla Pilao. Mais les menaces ont sensiblement évolué. En ligne de mire à présent les terminaux point de vente, les fameux *Point of Sale* (PoS), majoritairement sous Windows XP dont on connaît la vulnérabilité. Ils permettent des détournements d'argent importants. Est aussi visé le secteur de la santé, pour le vol de données personnelles. Enfin, les mobiles sont devenus les principales cibles des pirates qui s'y installent par le biais du téléchargement de fausses applications.

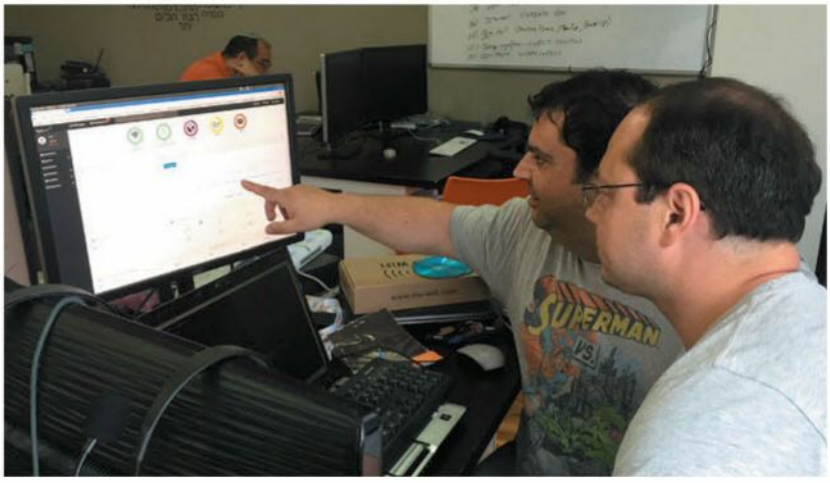


YadWire

Dynamiser la monétisation du WiFi

La start-up israélienne se présente comme un pionnier de l'injection de contenus publicitaires sur les réseaux WiFi publics.

La grand-messe du réseau sans fil, « Wi-Fi Now », qui se tiendra du 17 au 19 novembre à Amsterdam, sera l'occasion de le rappeler : la monétisation du WiFi fait partie des nouvelles frontières du secteur. Tel est aussi le cœur de cible de la start-up YadWire. Fondée en 2013 dans la région de Tel-Aviv par deux entrepreneurs français, David Ziza et Stéphane Hercot. Ce dernier, éditeur de logiciels WLAN, se présente comme un pionnier de l'injection de contenus publicitaires sur les réseaux WiFi publics. Le concept est simple : à l'heure où le WiFi se démocratise dans les lieux publics, YadWire propose aux entreprises de valoriser cette manne. *« Nous avons développés des modules d'injection via WiFi, qui permettent d'afficher du contenu aux utilisateurs tout au long de leur session »*, explique David Ziza, le PDG de YadWire. *« Nos technologies brevetées transforment ainsi tout WiFi public en espace informatif, publicitaire et interactif, notamment au sein de grandes installations comme les stades, les aéroports, les centres commerciaux ou encore les hôtels »*. La jeune entreprise, qui a commercialisé sa plate-forme en janvier 2014, revendique 70 000 injections de contenu en première année de lancement, et dessert plus de 7 000 hotspots WiFi dans le monde. *« Nous sommes à ce jour le seul spécialiste à offrir une technologie aussi flexible »*, assure le fondateur de YadWire, qui relève que le marché du nouveau standard d'authentification Hotspot.02, permettant d'interconnecter un grand nombre de points d'accès WiFi au travers d'accords d'itinérance, est en plein bouleversement.



Un marché très disputé

Il est vrai que les enjeux sont de taille. D'ici à la fin 2016, relève la jeune pousse, 84 % des hotspots appartiendront à la nouvelle génération, selon les chiffres de la Wireless Broadband Alliance. Tandis que l'usage de données issues des réseaux sans fil est en plein essor, puisque l'on estime qu'il sera multiplié par douze en 2019 comparé à 2013. Enfin, le marché mondial du WiFi devrait atteindre 26 milliards de dollars dans les quatre prochaines années. De quoi inciter de nombreux éditeurs à creuser le filon. YadWire arrive en effet sur un marché très disputé. Parmi ses principaux concurrents, on peut citer PurpleWiFi – dans lequel a investi l'ex-patron de Tesco, géant de la distribution britannique –, Front Porch, Socifi, Cloud9, Cloud4Wi ou encore RaGaPa.

La jeune pousse qui s'est financée à hauteur de 1,5 million de dollars auprès d'investisseurs privés, y compris les fondateurs, espère toutefois faire la différence grâce à ses outils permettant un marketing ciblé et en temps réel, l'utilisateur du WiFi étant identifié (sexe, âge) et pouvant être géo-localisé sous différents formats (SMS, vidéo, etc.). Elle propose ainsi des analyses de données avancées garantissant l'impact des campagnes de communication. Sans oublier une active politique de partenariat qui l'a notamment conduit à collaborer avec Orange Horizon, sur le déploiement de réseaux WiFi en Afrique du Sud, et TDF dans l'événement sportif. ✖

Nathalie Hamou

5ème édition

mobility for business

6 - 7 - 8 OCTOBRE 2015
PARIS
PORTE DE VERSAILLES

Le salon des solutions, applications et terminaux mobiles pour les entreprises

4 000 visiteurs professionnels
130 exposants
50 conférences et ateliers
4 Keynotes
1 soirée Networking

New !

- **Des rendez-vous projets**
- **Focus Security for Business**
- **1ère édition des Mobility Awards**

Pour tout renseignement :
www.mobility-for-business.com

Sponsors Platinum

Motion by XPLORE
praxedo Solution Cloud de gestion d'interventions

Partenaire Media

L'INFORMATICIEN

SOLUTIONS SALONS erp

18ème édition

EXPOSITION
CONFÉRENCES
TABLES RONDES
ATELIERS
RENDEZ-VOUS
PROJETS

Le salon des progiciels de gestion intégrés

POUR LES GRANDES ENTREPRISES ET LES PME - PMI

- ADMINISTRER LES GRANDES FONCTIONS
- PILOTER L'ACTIVITÉ EN TEMPS RÉEL
- FIDÉLISER LES CLIENTS
- DÉVELOPPER SES MARCHÉS
- INTÉGRER LES SOLUTIONS
- MODERNISER L'ENTREPRISE ...

6*• 7 • 8 octobre 2015
PARIS EXPO
PORTE DE VERSAILLES

*(à partir de 14h00)

www.salons-solutions.com

En parallèle

SOLUTIONS SALONS démat
SOLUTIONS SALONS crm
SOLUTIONS SALONS bi
SOLUTIONS SALONS e-achats
SOLUTIONS SALONS serveurs & applications

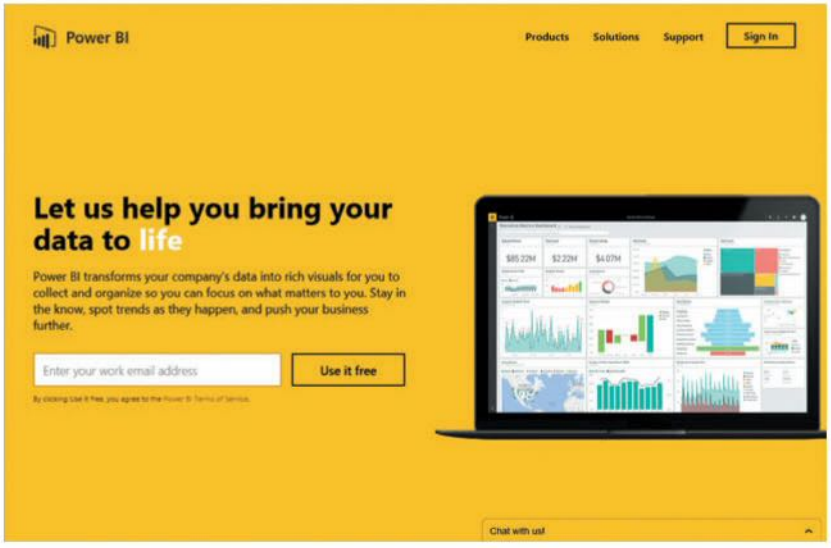
Votre meilleur outil de développement commercial !

Power BI 2.0 : une Self-BI immédiate et accessible

Durant l'été, Microsoft a officialisé la première mise à jour majeure de sa « Self-BI » en ligne, Power BI. Cette nouvelle version permet à la solution d'être plus indépendante d'Excel et d'Office 365 et la rend surtout beaucoup plus accessible à toutes les entreprises… Et il y a même une version gratuite !

Depuis quelques années déjà, la Self-BI est devenue la priorité stratégique de Microsoft en termes d'outils analytiques. Celle-ci s'est essentiellement forgée autour d'Excel et de SQL Server au travers de plugins Excel qui ont, petit à petit, forgé l'offre Microsoft : PowerPivot – outil d'analyse et de gestion de vastes collections de données introduit avec SQL Server 2008R2 –, Power View – outil de visualisation interactif et dynamique introduit avec SQL Server 2012 R2 –, Power Query – outil d'importation et d'exploration des données multi-sources. Microsoft a commencé quelque peu à désolidariser son approche BI d'Excel en introduisant l'an dernier son offre Power BI qui combinait les trois modules évoqués ci-dessus à quatre autres briques : Power Maps, pour la modélisation et l'affichage des données géolocalisées, Power Q&A, pour l'interrogation des données en langage naturel, Power Site BI, pour exporter et partager les rapports via un portail Web, et Power BI Admin Center, qui permet notamment aux administrateurs d'exposer les données on-premises sous forme de flux OData. Tous ces outils ne visaient qu'un seul objectif, rendre la BI accessible en « self-service » au plus grand nombre de collaborateurs possibles grâce à la convivialité des outils et leur intégration native au sein d'un espace maîtrisé de tous, Excel.

Pour essayer le service, allez sur "powerbi.com" et saisissez une adresse mail professionnelle.



Une approche différente

Avec Power BI 2.0, lancé le 24 juillet dernier, Microsoft modifie son approche pour en corriger deux défauts majeurs : Power BI 1.0 ressemblait trop à un amoncellement d'outils indépendants et la solution s'adressait exclusivement aux utilisateurs d'Office 365 disposant d'Excel.
Deux défauts qui empêchaient cette Self BI de décoller d'autant qu'elle alourdissait de façon significative l'abonnement Office 365 de chaque collaborateur.
Avec Power BI 2.0, Microsoft repart à l'attaque avec une agressivité retrouvée. Non seulement la solution est aujourd'hui bien plus unifiée, mais elle prend aussi son indépendance aussi bien vis-à-vis d'Excel que d'Office 365. Avec, au passage, des tarifs très largement revus à la baisse puisque la solution peut aisément être expérimentée gratuitement et utilisée gratuitement au quotidien par des TPE et auto-entrepreneurs aux besoins collaboratifs réduits.
Il est important de noter que les anciens modules

De nouvelles formes de visualisation font leur apparition.

Excel restent d'actualité – et sont même intégrés en standard dans le futur Excel 2016. Ils restent en effet plus cohérents avec une approche BI *« 100 % On Premises »* construite autour de SQL Server et des Data Warehouses locaux de l'entreprise.

Car l'approche « Power BI 2.0 » est avant tout une solution cloud davantage pensée et imaginée pour des analyses sur des structures de données relativement simples, même si une fois assemblées les différentes sources, la structure finale peut s'avérer assez complexes, et des sources de données principalement stockées dans le Cloud. La force de la solution est de ne nécessiter aucune « expertise » pour mettre en œuvre cette BI, faire parler ses données en les associant éventuellement à différentes sources web et réaliser ses tableaux de bord. Power BI 2.0 est une BI qui se veut simple et efficace. Une approche qui n'est pas nouvelle sur le marché, des solutions comme Qlik Sense allant nettement dans ce sens également.

Power BI Desktop

L'une des grandes nouveautés de Power BI 2.0 est sans conteste l'introduction d'un logiciel dénommé « Power BI Desktop », jusqu'ici connu sous le nom de Power BI Designer. Il permet de réaliser des analyses de bout en bout, de l'importation des données jusqu'à leur visualisation, sans avoir besoin d'Excel ! En pratique, c'est l'outil de conception des rapports et tableaux de bord. Il offre un canvas assez libre et ouvert sur lequel déposer vos données et choisir leur représentation.

Power BI Desktop est librement téléchargeable. Une fois le logiciel installé, vous pourrez vous connecter en quelques clics à vos sources de données – on-premises, Web, Cloud, feuilles Excel, etc. –, façonner les données selon vos besoins, visualiser les analyses sous forme de tableau de bord interactif et partager vos résultats de sorte que vos collaborateurs/partenaires puissent les afficher aussi bien sur un navigateur web qu'une app mobile, tout en conservant la même interactivité.

L'intérêt d'un tel outil installé sur son PC est déjà de pouvoir s'affranchir d'Excel dès lors que l'on ne veut que faire du reporting, mais surtout de pouvoir manipuler les données avec davantage de fluidité et de réactivité que sur un outil totalement web.

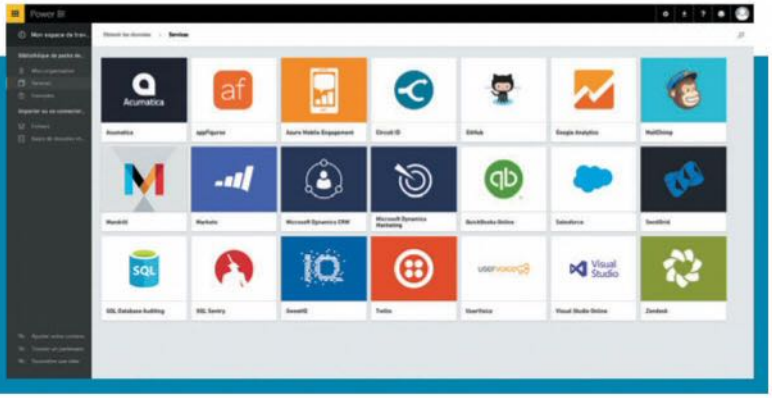
De nouvelles visualisations

Parmi les choses nouvelles introduites par Power BI Desktop, on notera l'apparition de nouvelles visualisations. C'est évidemment un aspect essentiel de toute Power BI. La représentation des données est l'étape ultime de toute analyse et le meilleur moyen de les rendre parlantes.

Microsoft introduit ici de nouveaux types de graphiques : Area Chart, Waterfall, Donut, Matrix.

Power BI Content Packs

Power BI ne s'alimente pas uniquement des sources de données reconnues en standard. Microsoft a ouvert sa plate-forme par le biais de Content Packs. N'importe quel fournisseur d'informations peut désormais proposer un accès depuis Power BI à ses sources de données en ligne et même fournir des tableaux de bord préfabriqués pour en simplifier l'accès. Notez que les entreprises peuvent également diffuser par ce biais leurs propres sources de données et rapports afin de mieux contrôler l'usage et l'accès des utilisateurs aux informations ainsi exposées.



La page d'accueil du portail Power BI une fois que vous êtes enregistré.

L'ensemble peut être enrichi de légendes, d'effets de couleurs, d'images importées placées en illustration ou en fond, de commentaires textuels et d'hyperliens.

Il est aussi important de noter que Power BI est l'un des rares outils à ne pas être limités à ses seules visualisations : Microsoft a en effet ouvert le logiciel à des visualisations tierces et publié son framework d'affichage en open-source (cf. encadré).

Une fois les éléments assemblés, on peut sauvegarder le rapport sous forme de fichier local « .pbix ». Mais, dans la plupart des cas, on cherchera bien évidemment à communiquer et partager son rapport ou tableau de bord. Une icône dans la barre d'outils permet de directement publier le rapport sur le nouveau portail « Power BI ».

Un nouveau portail

Une fois le rapport publié sur le site « Power BI », il devient potentiellement accessible à vos collaborateurs et partenaires. Le nouveau portail web introduit la notion de « Groupes » et de partage entre « Groupes ». Ainsi, les différentes équipes ou les différents services peuvent aisément travailler sur les mêmes rapports, les mêmes tableaux de bord, les mêmes jeux de données, et collaborer autour de ces éléments et des informations mises en évidence.

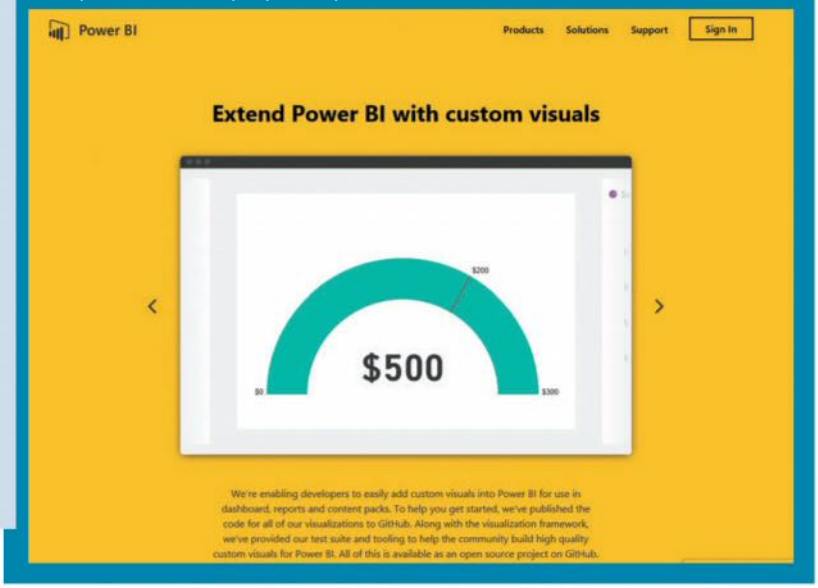
Une fois publiés, les rapports conservent tout leur aspect dynamique et interactif. On peut aisément naviguer dans les données, les sélectionner, les filtrer, etc. Mieux encore, il est possible de venir éditer les rapports et dashboards. Le nouveau portail offre en effet une version « webisée » de Power BI Desktop avec à peu près les mêmes fonctionnalités et la même ergonomie.

Notons également, qu'il est possible au travers de ce portail de publier des tableaux Excel, qui seront directement éditables du portail grâce à l'intégration d'Excel Online, et d'utiliser ces tableaux dans les analyses et rapports réalisés en ligne.

Des graphiques en Open Source

Microsoft a publié en Open Source le framework de visualisation sous-jacent à Power BI 2.0, qui s'appuie sur D3.js et Node.js. Tous les outils, codes et tests, sont disponibles sous GitHub : https://github.com/Microsoft/PowerBI-visuals.

Dès lors, les utilisateurs de Power BI ne sont plus limités aux seuls graphes et représentations proposés par Microsoft.



Des connecteurs Very Big Data

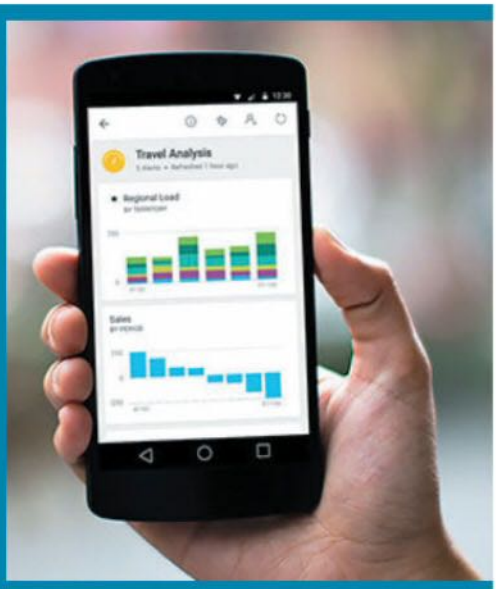
Power BI est une solution cloud en SaaS qui affiche une véritable vocation hybride. C'est visible au travers de la dichotomie des fonctions d'édition Power BI Portal/Power BI Desktop mais également au niveau de la connectivité et donc des sources de données exploitables.

Payant ou gratuit ?

Avec Power BI 2.0, Microsoft réinvente totalement la commercialisation de sa BI. L'arrivée de Power BI Desktop met davantage la solution Microsoft en comparaison frontale avec les stars des solutions de visualisation et plus particulièrement Tableau Software et Qlik Sense qui offrent toutes deux une édition communautaire gratuite. L'accès gratuit au portail Power BI et à son éditeur de rapport sous Windows, permet à Microsoft de venir jeter un gros pavé dans cet univers, d'autant que la version gratuite donne aussi accès aux outils Power BI Mobile.

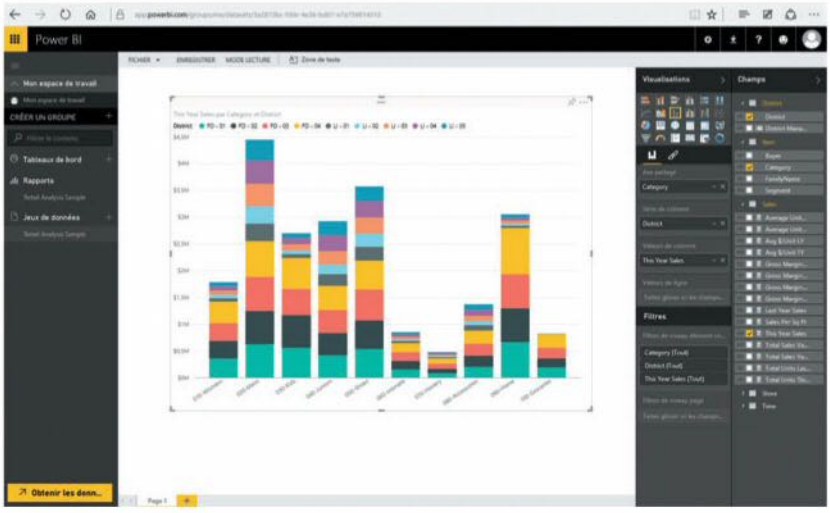
Mais même avec une version "Pro" à 9,99 $/mois/utilisateur, la nouvelle mouture se montre beaucoup plus économique que l'ancienne, d'autant qu'elle n'est plus rattachée à Office 365. Cet abonnement mensuel offre accès aux fonctions collaboratives du portail, avec une synchronisation des groupes Active Directory pour un management hybride, et libère les limites de mises à jour des rapports via streaming (1 million de lignes/heure contre 10 000 lignes/heure pour la version gratuite) et de stockage (10 Go contre 1 Go pour la version gratuite). Par comparaison, la solution d'IBM "Watson Analytics", très similaire dans l'esprit, est facturée 30 $/utilisateur/mois.

La BI se fait mobile



Les rapports et dashboards publiés sous Power BI 2.0 peuvent aisément être affichés sur n'importe quel navigateur web en conservant toute leur interactivité, quel que soit le dispositif. Mais Microsoft a poussé le raisonnement encore plus loin et fournit également avec Power BI 2.0 des applications mobiles simplifiant l'accès aux publications. Celles-ci permettent de facilement annoter les rapports, de partager ses analyses, de regrouper les visualisations clés au sein de tableaux de bord mobiles. Outre les apps Windows Phone/Windows 8, iPad et iPhone déjà disponibles, Microsoft a également publié en août la version Android.

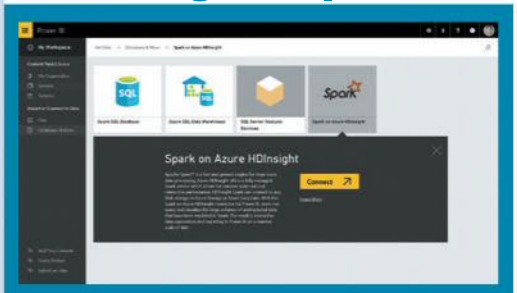
Microsoft joue à fond la carte de la simplicité et de l'ouverture avec la possibilité d'intégrer, simplement en quelques clics, des sources de données aussi variées que Salesforce, Marketo, ZenDesk, GitHub, Visual Studio Application Insights, Dynamics CRM, SendGrid, QuickBooks Online. Là encore, Microsoft joue la carte de l'ouverture n'importe quel service pouvant venir greffer son connecteur dans Power BI. Ainsi, plusieurs autres connecteurs sont déjà annoncés dont : Analytics, comScore, Azure Mobile Engagement, Sage, SpaceCurve, tyGraph, CircuitID, Sumo Logic, SQL Sentry, Zuora, Planview, Insightly, Troux, Inkling, etc.



Édition de rapport à partir de l'interface web.

On notera au passage qu'il n'est pas nécessaire d'importer les données puisque la solution permet de définir des liens persistants qui se mettent à jour à des périodes définissables – qui dépendent de l'abonnement, la version gratuite étant limitée à une mise à jour par 24 heures.
Bien évidemment, tout ce qui provient d'Azure est aussi directement intégrable qu'il s'agisse de toute la solution Azure Data Factory, des bases de données Azure, de Azure HDInsight (cf. encadré Spark), des flux d'Azure Stream Analytics, et des nouveaux services Azure DataWarehouse et Azure Data Lake.
Enfin, un connecteur relie également Power BI à vos intances « on-premises » de SQL Server Analysis Services. Les rapports et Dashboards interrogent alors directement les données locales. On peut explorer les models tabulaires d'Analysis Services depuis Power BI et conserver une connexion « live » afin d'éviter d'avoir à importer les données et conserver des vues toujours actualisées.
Enfin, sachez qu'il est aussi très facile d'importer des données provenant d'un tableau Excel stocké sur un disque en ligne OneDrive, un point fondamental pour les TPE qui auront adopté Windows 10 et pris l'habitude de tout stocker sur le stockage en ligne intégré au cœur du système, d'autant que durant l'été Microsoft a mis

HDInsight Spark



Bien évidemment, les utilisateurs de Power BI peuvent se connecter directement à Azure SQL Database, Azure Data Lake, Azure SQL Data Warehouse en bénéficiant de la même souplesse de requêtage direct « live » que ce qui existe avec SQL Server Analysis Services. Mais Microsoft a également lancé durant l'été la version preview de *« Spark for Azure HDInsight »*. Une solution bien évidemment connectée à Power BI qui dispose ainsi d'un accès Big Data pour afficher des tableaux et rapports interrogeant en direct les données Spark.

SALON 100 % PROFESSIONNEL, 100% SOLUTIONS CONNECTÉES

15|16 SEPTEMBRE 2015
CITÉ INTERNATIONALE LYON

i-Connect

LES RENCONTRES DE L'OBJET CONNECTÉ

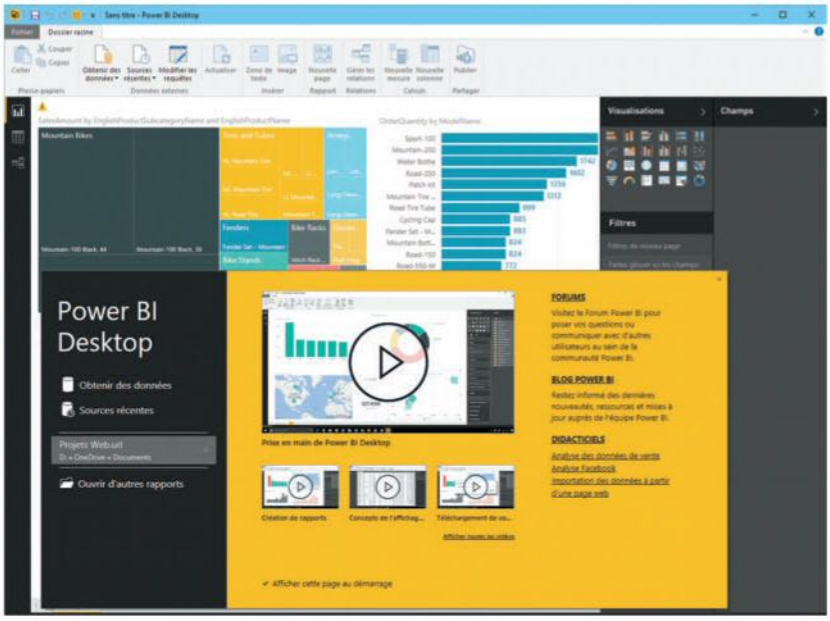
L'ÉVÉNEMENT BtoB

qui rassemble tous les acteurs
de la conception et fabrication
DES OBJETS CONNECTÉS

VOUS AUSSI,
POSITIONNEZ-VOUS EN ACTEUR CLÉ !

Plus d'informations :

www.iconnect-exhibition.com / Tel. 04 74 73 16 84

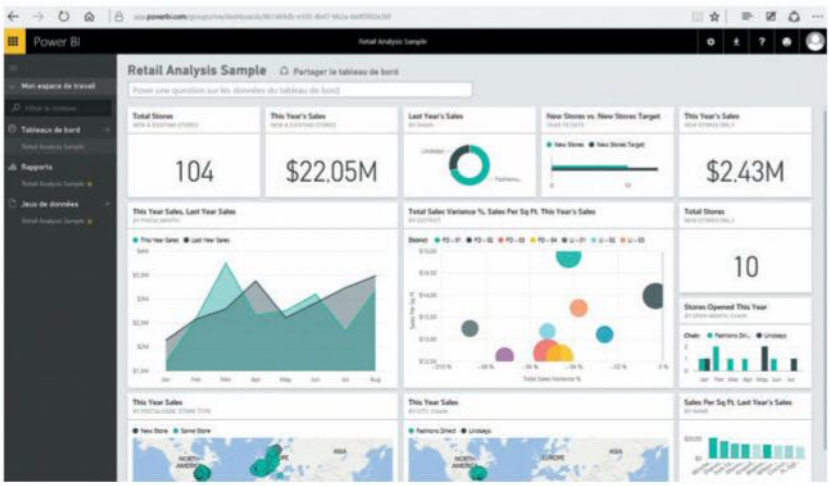


Power BI Desktop, autrefois connu sous le nom de code Power BI Designer, permet une conception plus réactive et plus productive des rapports et dashboards.

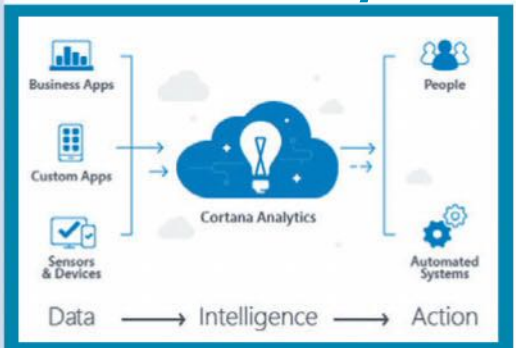
à jour OneDrive pour offrir une solution de dossier partagé en ligne hyper pratique.
En bref, force est de constater que Microsoft a déployé beaucoup d'énergie pour faire de Power BI une solution à la fois simple, accessible et plutôt complète. La facilité et la liberté de création offertes rappellent celles de solutions ultra ergonomiques et novatrices, dont Qlik Sense par exemple. Les PME et TPE apprécieront l'approche SaaS et la simplicité générale non seulement des outils, mais aussi de l'administration au travers des groupes. Les grandes entreprises seront en revanche probablement plus frileuses à moins d'avoir déjà largement opté pour le Cloud et Office 365. Si toutes les sources de données sont demeurées « on-premises » avec de fortes contraintes de surveillance et de contrôle, la mise en œuvre de ce Power BI 2.0 nécessitera une remise en cause des mentalités et de l'infrastructure. Elles auront toutefois de plus en plus de difficulté à faire abstraction des gains induits par le fait qu'il n'est plus désormais nécessaire de disposer d'Office 365, de Sharepoint et des ressources IT associées pour accéder à cette self-BI. Sans compter que chacun peut désormais jouer avec et se l'approprier gratuitement. ✖

LOÏC DUVAL

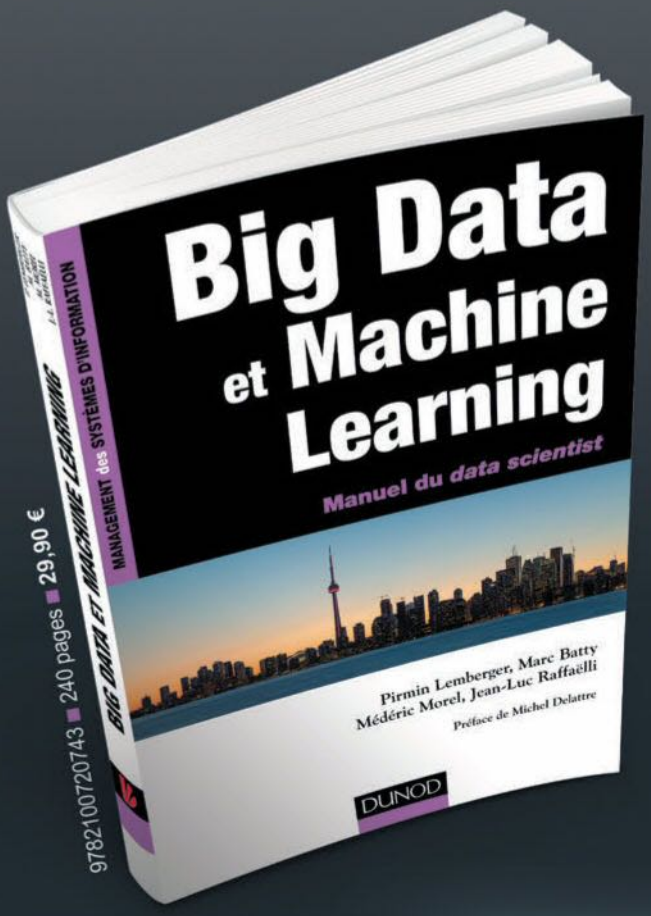
L'espace de travail du portail Power BI met en évidence les rapports, tableaux de bord et jeux de données disponibles et partagés.



Cortana Analytics

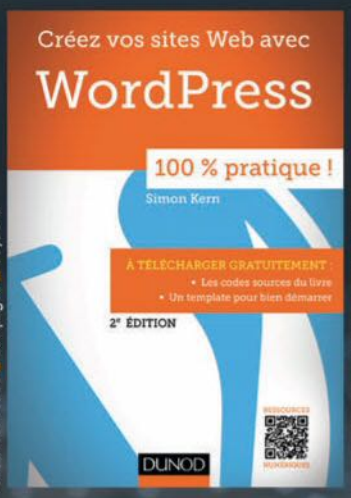


Décidément, l'été aura été très actif chez Microsoft. Outre la sortie de Power BI 2.0, de Windows 10 et d'une floppée de services Azure, l'éditeur a également levé le voile sur une innovation : Cortana Analytics Suite. Il s'agit d'un service sur abonnement qui regroupe tous les services analytiques de Power BI 2.0, plus ceux d'Azure (Data Factory, Data Lake, Stream Analytics, Machine Learning), en y ajoutant une surcouche d'intelligence artificielle patronnée par l'assistante virtuelle Cortana.
Il devient dès lors possible d'interroger directement les données en vocal, la reconnaissance linguistique de Cortana étant connectée au moteur d'interrogation en langue naturelle Power BI Q&A. Les résultats s'affichent directement sous forme de graphiques et rapports dans le volet Cortana. Mais l'assistante ne sert pas uniquement d'interface vocale. Elle apporte aussi tous les services d'Intelligence Perceptuelle qui lui sont liés – certains étant liés au Projet Oxford de MS Research comme la reconnaissance faciale. Elle apporte aussi un ensemble de scénarios préconfigurés pour des métiers donnés comme la maintenance préventive, la détection de fraude, les services médicaux, le manufacturing, etc.
Avec Cortana Analytics Suite, Microsoft semble vouloir concurrencer les solutions de « Big Data as a Service », dédiés à des domaines précis, qui se multiplient ces derniers mois sur le Cloud américain en y adjoignant le visage familier de son assistante virtuelle.



Le guide pour comprendre les enjeux d'un projet **Big Data** et mettre en place un **data lab**

À DÉCOUVRIR ÉGALEMENT



www.dunod.com

DUNOD
ÉDITEUR DE SAVOIRS

Qt 5.5, quoi de neuf sous le soleil ?

Nous vous avions parlé dans un précédent article d'une bibliothèque graphique pour le langage C++ qui était au-dessus de la mêlée : le framework Qt, prononcez *Cute*, (donc "quioute"), est sorti dans sa version 5.0 en 2012. Et la 5.5 vient juste d'être finalisée. Nous allons voir quels sont ses apports et en quoi celle-ci constitue une version incontournable, sans pour autant représenter une rupture totale depuis la version 4.

Qt est un framework orienté objet et développé en C++ par Haavard Nord et Eirik Chambe-Eng. Née sous le nom de Quasar Technologies en 1994, devenue ensuite Trolltech et Nokia – via ses filiales Qt Software puis Qt Development Frameworks) –, le code de Qt a changé plusieurs fois de propriétaire et de type de licence (GPL puis LGPL/commerciale). Il arbore aujourd'hui le pavillon Digia, qui assure que les sources du projet resteraient à disposition de tous, c'est à dire de la communauté. Qt met à disposition des composants d'interface graphique, à base de widgets et du QML, mais aussi d'accès aux données, de connexions réseau, de gestion des fils d'exécution, d'analyse XML et bien d'autres. En plus d'une librairie de code, Qt est aussi un framework de développement et un EDI (environnement de développement intégré) grâce à son outil Qt Creator. Cette évolution de la bibliothèque graphique C++ la plus populaire est considérée comme majeure pour la plupart des développeurs. Malgré d'importantes évolutions, elle a été conçue afin d'assurer au mieux la rétrocompatibilité avec la version 4, comme cela avait été le cas lors du passage de la version 3 à la 4. La plupart du temps, il suffit de modifier légèrement le .pro et les inclusions d'un projet développé en Qt 4 puis de le recompiler.

Digia, the Qt Company, possède désormais l'intégralité du code Qt et en gère le support.

Une bibliothèque graphique pleine de ressources

Qt n'est pas seulement une bibliothèque graphique multi plate-forme. Elle offre bien d'autres fonctionnalités :

- une abstraction de certains types et structures de données qui vient enrichir celle du C++ ;
- des composants graphiques standard prêts à l'emploi sous forme de classes et de boîtes à outils de widgets (QtDesigner) ;
- l'accès direct et la manipulation de bases de données ;
- des moyens de communication pour les réseaux IP ;
- des fonctionnalités multimédias ;
- la possibilité d'utiliser différents formats web : HTML, XML, JSON ou SVG.
- l'affichage et l'écriture de fichiers graphiques et de documents au format ODF ;
- une gestion fine des traductions ;
- un système de gestion d'événements via le concept de signaux et de slots, qui sont une implémentation du patron de conception observateur.

Son côté multi plate-forme va bien au-delà du simple trio Windows, Mac OSX et Linux/X11 sur x86 avec la gestion de Wayland, le nouveau protocole graphique en passe de remplacer X11. Cela ouvre les portes de la programmation

Pour tout savoir sur Wayland, le successeur de X, rendez-vous sur freedesktop.org.

graphique pour ARMv7, confirmant l'orientation prise vers le monde de l'embarqué. Le support de X11 a été modifié pour passer de Xlib à XCB.
Parmi les nombreux ajouts qui ont été réalisés, il faut notamment citer :

- la gestion du DNS alors que Qt 4 ne gérait que la résolution de nom ;
- un lecteur et générateur JSON ;
- la gestion des types MIME, sur extension et sur contenu, y compris en mémoire ;
- la prise en charge des souris de gamer, avec un nombre de boutons adapté à l'interface graphique (jusqu'à 27 sous X) ;
- la prise en charge des nouveautés de C++ 11, si bien entendu le compilateur C++ est compatible.

Un développement qui reste ouvert à tous

Depuis le 9 août 2012, Digia est le nouveau propriétaire de l'ensemble de la bibliothèque. L'entreprise finlandaise disposait déjà du droit exclusif de vente de licence commerciale et gérait le support payant, mais Nokia conservait encore la propriété de l'ensemble du code source de Qt et décidait de son évolution. Nokia avait racheté Trolltech en 2008 et cédé la partie commerciale à Digia en 2011. Digia a récemment annoncé vouloir renforcer l'équipe de développement de Qt afin de porter rapidement la bibliothèque sur les principaux systèmes d'exploitation mobiles (Android, iOS et Windows 8), sans pour autant relâcher son attention de la version Desktop. 125 développeurs de l'équipe R&D consacrée par Nokia à Qt auraient été réembauchés par Digia. Le développement de la bibliothèque reste ouvert à tous et le système à double licence, LGPL et commerciale, est préservé.
D'autres acteurs économiques sont liés à Qt, outre les grandes entreprises qui l'utilisent depuis des années pour leur code. La société Jolla, fondée par des anciens développeurs du projet Meego de Nokia, a repris la partie embarquée de Qt et projette de sortir prochainement du matériel sous Sailfish OS. RIM a utilisé Qt pour créer l'interface de son Blackberry 10.
Digia continue de supporter le site communautaire du projet Qt (http://qt-project.org/) sur lequel vous trouverez les différentes règles concernant l'ajout de code à Qt. Le code source est disponible dans son intégralité et géré avec Git. Un système élaboré de relecture de code utilisant Gerrit a été mis en place. Le développement reste donc ouvert à toutes les bonnes volontés, avec un accès au code facilité et une politique d'inclusion publique. L'inquiétude de voir le projet Qt sortir de l'Open Source semble donc s'être éloignée, du moins pour le moment. Le développement de Qt devrait suivre un processus basé sur une version livrée à peu près tous les six mois. Les fonctionnalités sont développées dans des branches. Ce qui est considéré comme stable au moment du gel de la version sera inclus dans la version mineure suivante.

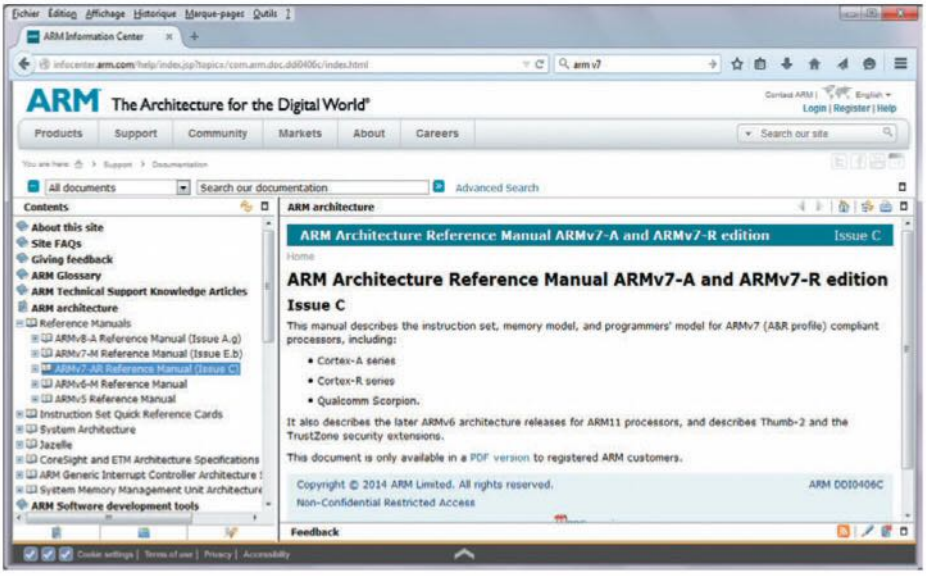
Modularisation

Le nombre de fonctionnalités de Qt devenant de plus en plus important, le code source a été réparti dans plusieurs dépôts, et ce, de manière à en faciliter le développement. Le code de QtQuick ou celui de QtWebkit, par exemple, ne font plus partie du même dépôt que les bibliothèques de base.

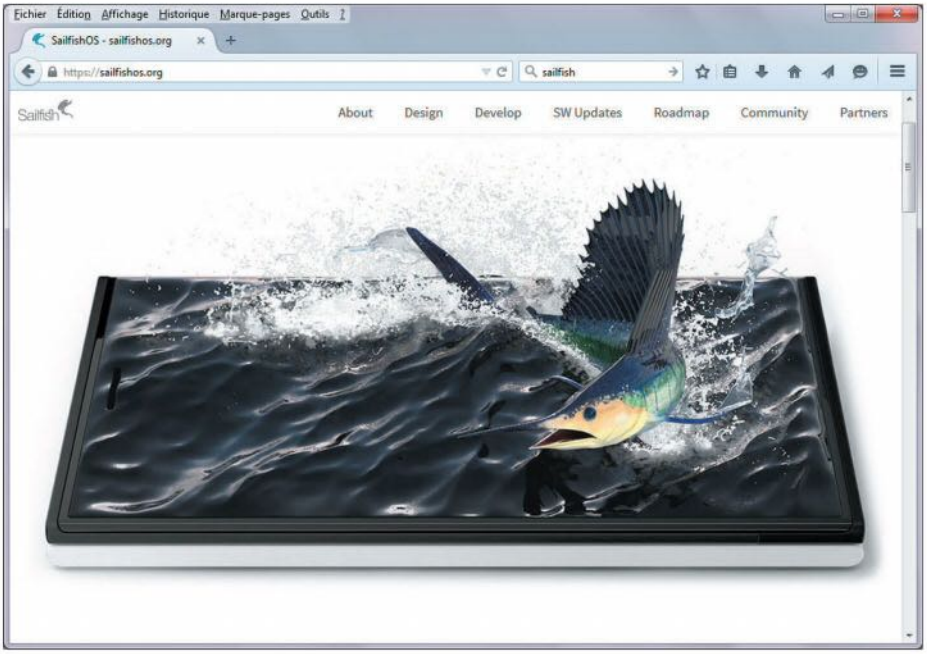
Rétro-compatibilité du code source

Digia a fait en sorte que Qt 5 préserve au maximum la compatibilité avec le code source développé en Qt 4. Le portage d'application reste effectivement

C'est Gerrit qui a été retenu pour la révision du code de Qt.



ARM v7 : l'architecture de prédilection pour l'embarqué.



Sailfish OS, le système d'exploitation pour plates-formes mobiles, basé sur le noyau Linux et développé par la société finlandaise Jolla.

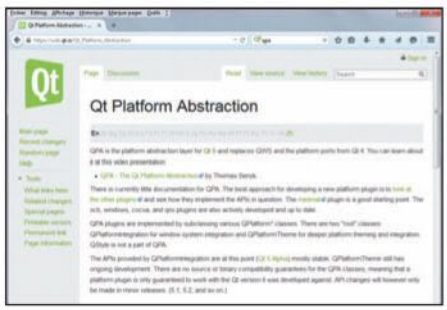
relativement simple, même s'il ne consiste pas, comme l'aurait voulu l'entreprise, en une simple recompilation.

Le système d'abstraction de Qt

QPA (Qt Platform Abstraction), qui a vu le jour avec Qt 4.8, est une couche d'abstraction destinée à faciliter le portage de Qt sur différentes plates-formes via des plugins, afin surtout d'éviter l'insertion de #ifdef dans le code. QPA est utilisé par défaut sur toutes les plates-formes, dont bien sûr Windows, Mac OS X et Linux. Sous Linux, c'est encore XCB qui est utilisé par défaut pour la communication graphique avec le serveur X11. Il existe néanmoins un plugin pour Wayland, le système d'affichage recommandé pour l'embarqué. QPA sert aussi de base au portage vers iOS, Android et Windows 8 mobile. Ces derniers sont officiellement supportés par Digia depuis la version 5.1 de Qt.

Le langage QML et QtQuick 2.0

QtQuick représente une des principales évolutions de Qt. QML, introduit dans Qt 4.7, est un nouveau langage de description d'interface pour Qt. Il utilise le langage Javascript. QtQuick désigne l'ensemble des technologies tournant autour de QML. La version 2.0 de Qt Quick comportant d'importants changements, elle n'est pas du tout compatible avec QtQuick 1.x. Digia fournit, fort heureusement, un module de compatibilité pour permettre aux applications écrites avec Qt 4.x et utilisant QML de fonctionner sous Qt 5. Le principal changement affectant QtQuick 2.0 est la réécriture du moteur d'affichage. Celui-ci utilise un graphe de scène (scenegraph) basé sur OpenGL. Le rendu étant effectué dans un thread (processus léger) séparé, les animations complexes en termes de graphisme sont plus fluides. Le moteur JavaScript de QML a lui aussi été changé. Qt 5 utilise V8, le moteur JavaScript de Google, au lieu de QtScript qui utilisait lui JavaScriptCore. L'API de V8 est bien plus stable sur la durée que celle de Qt Script. Qt 5 propose donc, de fait, Webkit et Webkit2, aux API totalement incompatibles. Les navigateurs développés à l'aide de Qt 5 et surtout de Webkit2 devraient pouvoir concurrencer sérieusement les Firefox, Safari et autres Chrome. À tout cela s'ajoute encore les Components pour desktop, des éléments QML incluant une espèce de toolkit pour créer des applications de bureau.



QPA, le système d'abstraction de Qt destiné à faciliter le portage de Qt sur différentes plates-formes via des plugins.

Une syntaxe simplifiée pour les signaux et les slots

Une nouvelle syntaxe fait son apparition pour l'utilisation des signaux et des slots. Voici "l'ancienne" syntaxe, c'est-à-dire celle utilisée avec Qt 4 :

```
connect(sender, SIGNAL(valueChanged(QString,QString)), receiver, SLOT(updateValue(QString)));
```

Le souci avec cette manière de faire tient en ce qu'il n'y a aucune vérification lors de la compilation quant à l'existence des fonctions spécifiées. Le problème – si problème il y a – ne sera visible qu'à l'exécution. Attention donc aux fautes de frappe, elles peuvent être fatales. Une nouvelle syntaxe apparaît donc avec Qt 5. L'ancienne fonctionne toujours, nul besoin de modifier le code déjà écrit. Cela donne quelque chose de ce style :

```
connect(sender, &Sender::valueChanged, receiver, &Receiver::updateValue);
```

Avec cette syntaxe, le compilateur peut lever une erreur si la fonction n'existe pas. Il est également possible d'utiliser typedef et namespace ou d'avoir une conversion de type (cast) automatique (via le mécanisme d'inférence de type). Un signal envoie, par exemple, un QString et le slot récupère un QVariant. Le compilateur se débrouille pour adapter le type en fonction de l'entrée – ici QString. N'importe quelle fonction peut maintenant être utilisée comme slot. La déclaration explicite est toujours possible, mais elle n'est plus indispensable. Vous pouvez même utiliser une fonction lambda comme slot, ce qui ouvre les portes de la programmation

asynchrone :

```
connect(sender, &Sender::valueChanged, [=](const
QString &newValue) {
    receiver->updateValue("senderValue", newValue) ;
}) ;
```

La connexion de pointeurs de fonctions est similaire à une connexion classique, en donnant un pointeur sur les objets et sur les fonctions. Les classes émettrices et réceptrices doivent dériver de QObject mais sans qu'il soit nécessaire de déclarer les fonctions avec le mot clé slots.

```
    class Sender : public QObject {
  Q_OBJECT

signals:
  void send(int i = 0);
};

class Receiver : public QObject {

public:
  void receive(int i = 0) { std::cout &lt ; &lt ; &quot ;
receive:&quot ; &lt ; &lt ; i &lt ; send(123) ;
```

L'avantage de cette écriture est, encore une fois, que la validité des paramètres est vérifiée lors de la compilation et non lors de l'exécution.

Pour les fonctions lambdas :

```
    // connexion avec les lambdas
QObject::connect(s, &amp;Sender::send, [r](int i = 0) {
r-&gt;receive(i); }) ;
emit s-&gt ; send(456) ;
```

Dans ce code, le pointeur vers l'objet récepteur est capturé et le paramètre passé par la fonction send() est récupéré puis la fonction receive() est appelée dans le corps de la lambda. Le résultat obtenu est identique au code précédant, mais il est possible de faire beaucoup d'autres choses dans la lambda, comme par exemple de déconnecter tous les signaux d'un seul coup ou encore de parcourir tous les enfants de l'objet récepteur. Si le compilateur utilisé ne supporte pas les variadic template, les signaux et slots ne doivent pas avoir plus de cinq paramètres. Le système de signaux et slots de Qt5 semble avoir considérablement gagné en rapidité par rapport à son prédécesseur, que ce soit pour l'établissement de nouvelles connexions ou pour l'envoi de message.

Les modules de Qt 5

Les modules de Qt ont été complètement réorganisés dans la version 5. Ils sont désormais regroupés en deux groupes : les Essentials, qui sont installés automatiquement car totalement indispensables, et les Add-ons, installés seulement à la demande.

Les modules Essentials

Qt Core

Ce module fournit les fonctionnalités de base de Qt (comme c'est souvent le cas avec les "Core"), excepté en ce qui concerne l'interface graphique. Tous les autres modules lui sont liés. Voici la liste des ajouts apportés à Qt 5 :

- la classe QStandardPaths permet de récupérer les répertoires par défaut de la plate-forme. C'est une évolution de QDesktopServices, basée sur le modèle de KStandardDirs de KDE et avec plus de fonctionnalités. Cela permet par exemple de faire une recherche de toutes les occurrences d'un fichier dans les différents répertoires ;
- le support de JSON, ce qui permet de créer ou de lire un fichier JSON à partir d'une représentation binaire en mémoire ;
- extension de la prise en charge MIME, afin de permettre de déterminer le type mime d'un fichier ou de données en mémoire, en fonction de l'extension et/ou du contenu. Ce module utilise une base de données des types MIME via QMimeDatabase fourni par freedesktop.org shared-mime-info project. Cette base de données est incluse par défaut sous Linux. Elle est fournie par Qt sous Windows et Mac OS X ;
- la vérification des connexions signaux/slots à la compilation : vérifie l'existence du signal et du receveur et que les arguments sont compatibles. Cette fonctionnalité utilise les templates et est compatible avec C++ 11. Il est possible de connecter un signal à des fonctions lambda, des fonctions membres ou des fonctions statiques, sans avoir besoin de les déclarer comme slots :
- QRegularExpression : nouveau moteur d'expressions régulières compatible Perl, plus puissant et rapide que QRegExp, avec plus de fonctionnalités ;
- l'amélioration des performances, en particulier pour l'accès aux structures de données ;
- l'amélioration du support C++ 11 lorsque c'est possible, tout en préservant la compatibilité avec la norme C++ 98 ;
- le support des boutons supplémentaires sur les souris (souris pour joueurs), jusque 27 boutons pour XCB, XLIB ou DirectFB, jusque 16 pour Wayland, Evdev ou OS-X, jusque 8 pour BlackBerry/QNX et 5 sur Windows (limitation due au système).

Qt Gui

Le module Qt Gui fournit les classes et fonctionnalités de base permettant de créer une interface utilisateur riche en fonctionnalités. Il contient les nouvelles classes QWindow, QScreen, QSurfaceFormat essentiellement destinées à être utilisées par les autres modules (QWidget, QQuickView et autres Qt 3D View) ainsi que les classes QOpenGLxxx (QOpenGLFramebufferObject, QOpenGLShaderProgram, QOpenGLFunctions, QOpenGLContext et autres) qui fournissent l'accélération matérielle pour tous les modules graphiques (widgets traditionnels et Qt Quick). La classe QOpenGLContext, plus générique que QGLContext, est découplée de QWindow, ce qui permet d'utiliser un contexte commun pour plusieurs affichages. QOpenGLPaintDevice permet d'utiliser directement QPainter sur un contexte OpenGL sans avoir à dériver les classes QWindow ou QOpenGLFramebufferObject.

Qt Js (JavaScript) backend

Ce module fournit un interpréteur JavaScript qui permet de scripter les applications écrites en C++ et en QML. Il inclut de nouvelles classes telles

que QJSEngine ou QJSValue, le support de nouveaux types (QColor avec les propriétés r, g, b et a et QVector4D, constructible avec la méthode Qt.vector4d()). Il est possible d'ajouter des fonctionnalités dans un namespace avec la fonction qmlRegisterModuleApi et d'importer du QML et du JS directement dans un fichier javascript.

Le module Qt Quick

L'interface graphique de Qt Quick 2 se base maintenant, comme mentionné plus haut, sur scenegraph et permet l'accélération matérielle en utilisant les classes QOpenGLxxx de Qt Gui. Les nouvelles classes QQuickView, QQuickCanvas, QQuickItem et QQuickPaintedItem remplacent les classes équivalentes de QDeclarative. Canvas permet le support de l'API Context2D de HTML 5 en réalisant le rendu dans Canvas.Image et Canvas.FramebufferObject, avec support multithread en arrière-plan. Le moteur de particules 2D Qt Quick.Particles 2.0 et la collection d'effets de shaders ne sont plus des projets séparés de Qt Labs. Ils sont désormais directement inclus dans Qt.

Qt 3D

Le module Qt 3D est également un ancien projet provenant de Qt Labs. Il est enfin inclus dans Qt 5. Il a permis dans Qt 4 l'ajout de nombreuses fonctionnalités de calculs 3D avec les classes QMatrix4×4, QGLShaderProgram et QVector3D. Il utilise en interne le module Qt QML et le support OpenGL de Qt Gui. Ce module contient deux bibliothèques : Qt 3D (pour utiliser directement la 3D en C++) et Qt 3D Quick (pour l'utilisation dans Qt Quick). Qt3D ajoute la gestion d'objets 3D, des textures, des caméras, la possibilité de scripter du code 3D en QML et le chargement de fichiers .obj (fichier objet issu d'une compilation) et .3ds (3d studio).

Plusieurs fonctionnalités ont été ajoutées, dont principalement :

- la gestion de scènes 3D, avec rendu en OpenGL ;
- la lecture de fichiers 3D (.obj et .3ds) ;
- la gestion des lumières, des meshs, des textures, des matériaux, des animations, des caméras et des vues ;
- l'ajout de shader directement ou via le fichier de propriétés QML.

Qt Location

Le module Qt Location est, certes, un ajout de Qt 5, mais il existait déjà depuis de nombreuses années sous la forme d'un sous-ensemble du module Qt Mobility. Il fournit les services nécessaires à la localisation, du genre GPS ou cartographie. Il inclut une fonctionnalité d'affichage de cartes avec MapQuickItem. L'affichage est basé sur une approche modèle/vue et profite de l'accélération OpenGL dans scenegraph. La prise en charge des gestuelles pour les zooms et les panoramas dynamiques, le routage et le géocodage ainsi que l'ajout de repères sur les cartes est assurée.

Qt Network

Ce module, comme son nom l'indique, offre une interface multi plateforme permettant d'utiliser les réseaux. Parmi ses principales évolutions, citons notamment :

- l'amélioration du support IPv6 et de la gestion des réseaux IP en général. QTcpServer et QUdpSocket (lancés avec QHostAddress::Any) permettent de recevoir avec les deux protocoles de réception. QHostAddress::AnyIPv4 et QHostAddress::AnyIPv6 ne travaillent qu'avec un seul protocole. QNetworkAccessManager tente lui d'utiliser les deux protocoles (TCP, UDP). Il garde le premier qui "accroche" ;
- QTcpSocket peut désormais être attaché à un socket existant avant de lancer une connexion, ce en vue de limiter les connexions dans un environnement multi-hôte ;
- QDnsLookup sert à rechercher des enregistrements DNS. Sans remplacer QHostInfo, qui permet lui de résoudre les noms de domaine et autres URI en adresse IP, il donne accès aux autres types d'enregistrements DNS : SRV, TXT et MX ;
- les classes QFtp et QHttp ne sont pas conservées dans ce module, mais restent disponibles dans un module indépendant pour la rétrocompatibilité. Elles doivent être remplacées (dans le nouveau code) par QNetworkAccessManager ;
- les extensions et vérifications des certificats SSL : La vérification des certificats SSL ne se fait plus uniquement lors de la connexion à un serveur grâce à la nouvelle prise en charge des extensions des certificats ;
- le support des clés privées masquées pour lire une clé privée à partir d'un périphérique.

Les autres modules

- Qt Multimedia fournit les fonctionnalités de base pour lire l'audio, la vidéo, la radio et gérer les caméras ;
- Qt SQL offre fournit une prise en charge portable des bases de données SQL ;
- Qt Test fournit les outils indispensables à la mise en place des tests unitaires (très important avec Qt, car les plates-formes de test "classiques" pour le C++ ne sont pas adaptées) ;
- Qt WebKit est basé sur WebKit 2, mais sans changement de l'API C++. Ce module prolonge l'amélioration de la prise en charge du langage HTML 5 et des performances.

Les modules Add-ons

Le module Qt Widget

Ce module fournit l'ensemble des classes QWidget et dérivées pour la compatibilité avec Qt 4. Il utilise la nouvelle architecture QPA (Qt Platform Abstraction) dont nous avons parlé plus haut.

Le module Qt Quick 1

Ce module permet d'utiliser la version de Qt Quick disponible dans Qt 4, pour de pures raisons de compatibilité. Pour utiliser ce module, vous devez ajouter dans le .pro la ligne suivante : QT += quick1 et inclure dans le code le fichier d'en-tête : #include QtQuick/QDeclarativeView ✖

THIERRY THAUREAUX

Le magazine référence des développeurs

Kiosque | Abonnement

PROGRAMMEZ!

www.programmez.com

“Le cloud computing francais”

By Aspserveur

Faites-vous plaisir !

Prenez le contrôle du
premier Cloud français facturé à l'usage.

Autoscaling

Load-balancing

Metered billing

Firewalls

Stockage

Hybrid Cloud

Content delivery network

Content delivery network

Le CDN ASPSERVEUR C'EST

91 POPS *répartis dans*

34 PAYS

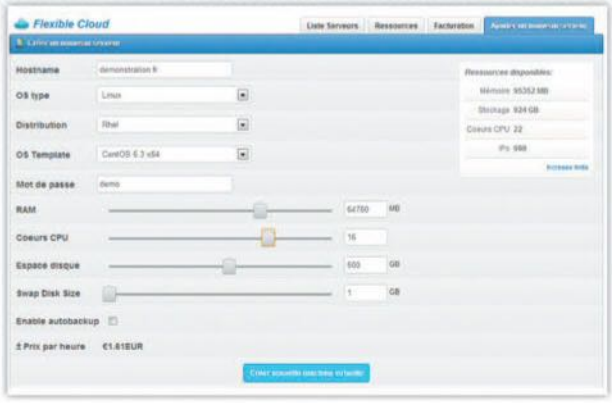
À partir de

0,03 €

(de l'heure)

Prenez le contrôle du 1er Cloud français réellement sécurisé...

Plus de 300 templates de VM Linux, Windows et de vos applications préférées !



Des fonctionnalités inédites !

Best management

Extranet Client de nouvelle génération, disponible pour la plupart des navigateurs, IPAD et ANDROID.

Facturation à l'usage

Pas d'engagement, pas de frais de mise en service. Vous ne payez que ce que vous consommez sur la base des indicateurs CPU, RAM, STORAGE et TRANSIT IP.

Best infrastructures

ASPSERVEUR est le seul hébergeur français propriétaire d'un Datacenter de très haute densité à la plus haute norme (Tier IV).

Best SLAs

100% de disponibilité garantie par contrat avec des pénalités financières.

Cloud Bi Datacenter Synchrone

Technologie brevetée unique en France permettant la reprise instantanée de votre activité sur un second Datacenter en cas de sinistre.

CDN 34 pays, 92 Datacenters

Content Delivery Network intégré à votre Cloud. Délivrez votre contenu au plus proche de vos clients partout dans le monde.

Geek Support 24H/7J

Support technique opéré en 24H/7J par nos ingénieurs certifiés avec temps de réponses garantis par contrat SLA (GTI < 10 minutes).

UNE EXCLUSIVITÉ ASPSERVEUR

ASP serveur

En savoir plus sur : www.aspserveur.com

ABONNEZ-VOUS À

Le magazine *L'INFORMATICIEN*

1 an / 11 numéros du magazine ou 2 ans / 22 numéros du magazine

Accès aux services web

L'accès aux services web comprend : l'intégralité des archives (plus de 140 parutions à ce jour) au format PDF, accès au dernier numéro quelques jours avant sa parution chez les marchands de journaux.

Bulletin d'abonnement à *L'INFORMATICIEN*

À remplir et à retourner à : **L'INFORMATICIEN - 38, rue Jean Jaurès 92800 PUTEAUX**

OUI, JE M'ABONNE À L'INFORMATICIEN ET JE CHOISIS LA FORMULE :

❑ Un an 11 numéros + l'ouvrage WINDOWS 10 + accès aux archives Web du magazine (collection complète des anciens numéros) en PDF : **49 €**

❑ Deux ans 22 numéros + l'ouvrage WINDOWS 10 + accès aux archives Web du magazine (collection complète des anciens numéros) en PDF : **87 €**

JE PRÉFÈRE UNE OFFRE D'ABONNEMENT CLASSIQUE :

❑ Deux ans, 22 numéros MAG + WEB : **87 €**

❑ Un an, 11 numéros MAG + WEB : **47 €**

❑ Deux ans, 22 numéros MAG seul : **79 €**

❑ Un an, 11 numéros MAG Seul : **42 €**

JE JOINS DÈS À PRÉSENT MON RÈGLEMENT :

❑ Chèque bancaire ou postal à l'ordre de *L'INFORMATICIEN*

❑ CB ❑ Visa ❑ Eurocard/Mastercard

N° ❑❑❑❑ ❑❑❑❑ ❑❑❑❑ ❑❑❑❑

expire fin : ❑❑/❑❑

numéro du cryptogramme visuel : ❑❑❑

(trois derniers numéros au dos de la carte)

❑ Je souhaite recevoir une facture acquittée au nom de :

_____

qui me sera envoyée par e-mail à l'adresse suivante :

_____@_____

JE SOUHAITE QUE MON ABONNEMENT À *L'INFORMATICIEN* DÉMARRE

avec le numéro : ❑ **139** (Octobre 2015) ❑ **140** (Novembre 2015)

J'INDIQUE LISIBLEMENT LES COORDONNÉES DU DESTINATAIRE DU MAGAZINE :

❑ M. ❑ Mme ❑ Mlle

Nom : _____ Prénom : _____

Entreprise (si l'adresse ci-dessous est professionnelle) :

_____

Adresse : _____

Code postal : _____ Ville : _____

Tél. : _____ Fax : _____

e-mail [*] : _____@_____

Secteur d'activité : _____ Fonction : _____

[*] Indispensable pour accéder à l'intégralité des archives de *L'INFORMATICIEN* sur *www.linformaticien.com* pendant toute la durée de votre abonnement.
L'INFORMATICIEN – Service Abonnements – 38, rue Jean Jaurès 92800 PUTEAUX, FRANCE Tél. : 01 74 70 16 30

Offres réservées à la France métropolitaine et valables jusqu'au 26/09/2015. Pour le tarif standard DOM-TOM et étranger, l'achat d'anciens numéros et d'autres offres d'abonnement, visitez *http://www.linformaticien.com*, rubrique Services / S'abonner Le renvoi du présent bulletin implique pour le souscripteur l'acceptation de toutes les conditions de vente de cette offre. Conformément à la loi informatique et libertés du 6/1/78, vous disposez d'un droit d'accès et de rectification aux données personnelles vous concernant. Vous pouvez acquérir séparément chaque numéro de *L'INFORMATICIEN* au prix unitaire de 5,40 euros (TVA 2,10 % incluse) + 1,50 euros de participation aux frais de port, l'ouvrage WINDOWS 10 au prix unitaire de 17,90 euros (TVA 5,5 % incluse) + 4,70 euros de participation aux frais de port et d'emballage. Pour toute précision concernant cette offre : abonnements@linformaticien.fr.

Pour toute commande d'entreprise ou d'administration payable sur présentation d'une facture ou par mandat administratif, renvoyez-nous simplement ce bulletin complété et accompagné de votre Bon de commande.

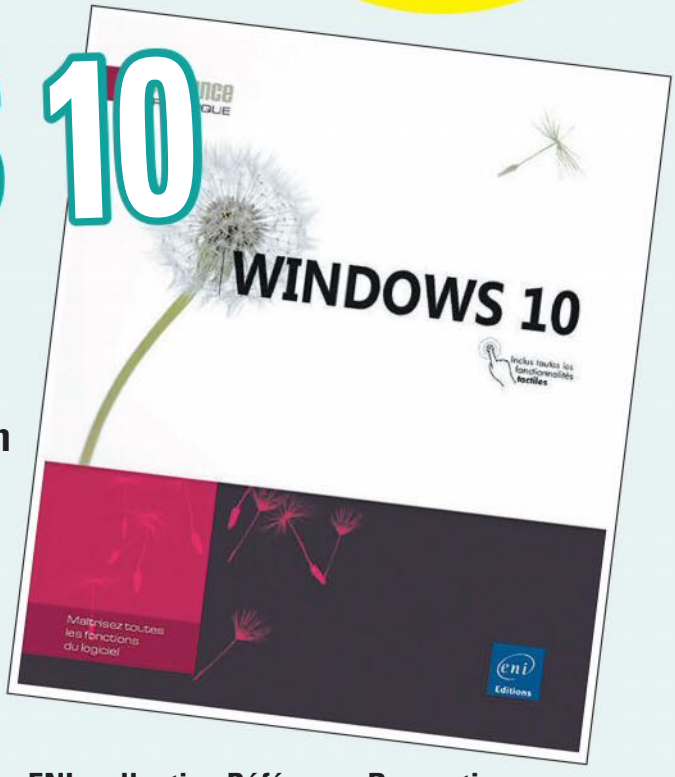
www.linformaticien.com
L'INFORMATICIEN

1 an d'abonnement 11 magazines + PDF

En cadeau avec votre abonnement

L'ouvrage WINDOWS 10

POUR SEULEMENT **49 €** AU LIEU DE 82 €*



Ce livre, l'un des premiers consacrés au nouveau système d'exploitation Microsoft, vous présente l'ensemble des fonctionnalités de Windows 10. Au sommaire : l'environnement de travail, la gestion de fichiers et des dossiers ainsi que de l'espace de stockage en ligne OneDrive, les recherches à l'aide de Cortana, les applications intégrées (notamment le nouveau navigateur Edge), les outils système…

Table des matières :
http://bit.ly/1I42DEk

Editions ENI, collection Référence Bureautique.
Livre (broché) - 17 x 21 cm - 320 pages - Niveau : Initié à confirmé
Date de parution : juillet 2015 - Version numérique offerte
Prix public : 17,90 €

** Prix des magazines achetés séparément (5,40 € x 11), ouvrage ENI (17,90 €), frais de port (4,70 €).*

Offert avec l'abonnement un an ou deux ans :
collection complète des anciens numéros de *L'INFORMATICIEN* en PDF

Offre réservée aux abonnés résidant en France métropolitaine. Quantité limitée. Frais de port inclus dans le prix. Offres valables jusqu'au 26/09/2015.
Pour toute information complémentaire merci de contacter le service diffusion à l'adresse abonnements@linformaticien.fr

Maîtriser WINDOWS 10

Ce qu'il faut absolument savoir

Windows 10 pille vos données personnelles, bloque vos jeux piratés (ou non) et renie votre carte graphique. Malgré tout, il squatte déjà près de 100 millions de PC et de tablettes, quatre semaines après son lancement. Le nouveau système d'exploitation de Microsoft ne doit pas être si terrible finalement... Puis vînt la question : « Comment l'utiliser correctement ? ». Ma mission, loin d'être impossible, consiste désormais à vous exposer nos conclusions. Évidemment, ces « trucs et astuces » ne sont pas parole d'évangile, il s'agit des petites choses de Windows 10 qui nous ont, depuis quelques semaines, simplifiée – ou pourrie – la vie.

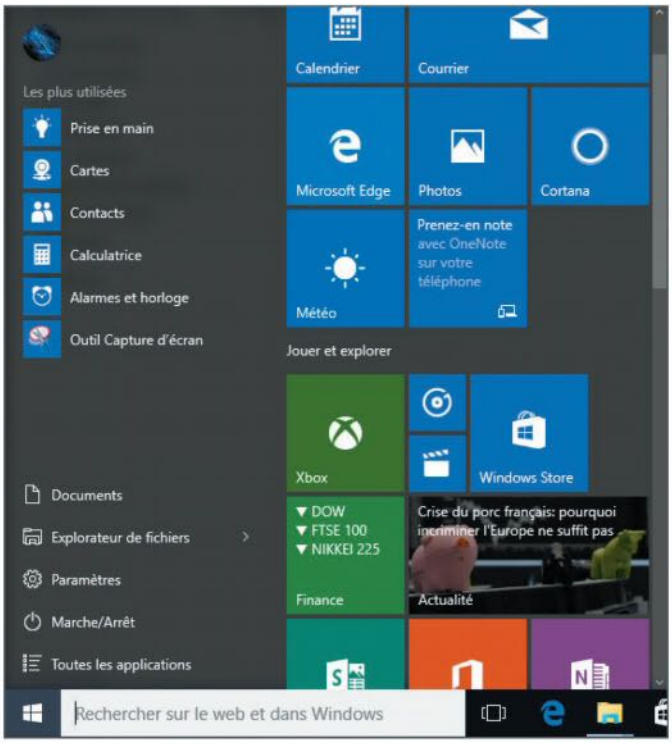
Start is back !

Le retour, plus beau que jamais, du menu Démarrer

« Enfin ! » Cri de triomphe de milliers d'utilisateurs alors que le menu Démarrer (le vrai, pas celui de Windows 8.1) revient sur Windows. À l'image de ses anciennes versions, le menu se divise en deux parties.

À ma gauche, par défaut, les icônes Paramètres, Marche/Arrêt et Toutes les applications. À ma droite, des tuiles dans un menu déroulant verticalement. Le ravalement de façade est total et mêle assez habilement, il faut bien le reconnaître, le meilleur des Windows 7 et 8. Du premier… le menu Démarrer et du second les tuiles. En effet, ces dernières sont personnalisables et je ne parle seulement que des trois ou quatre tailles de vignettes et de la possibilité de nommer les groupes de programme. Vous pouvez supprimer certaines icônes inutiles, les déplacer et, surtout, les désactiver – par clic droit ou glisser-déposer. Car les vignettes Xbox ou Assistant Mobile tournent en boucle, pire qu'un GIF… pour votre santé mentale, mieux vaut les figer.

Du côté gauche aussi, la personnalisation est de mise. Mais la manœuvre oblige à passer par les Paramètres de l'ordinateur, puis Personnalisation>Accueil. Là, vous pourrez décider d'afficher dans le menu Démarrer les applications les plus utilisées, celles récemment ajoutées ainsi que choisir les dossiers affichés dans l'écran d'accueil. Le choix est relativement limité mais permet de réintégrer au menu Explorateur de fichiers, Dossier personnel et Réseaux. En d'autres termes, trouver un programme est bien plus commode et rapide que sur Windows 8. Notons enfin qu'il est même possible de choisir la couleur du menu Démarrer. C'est un peu inutile, mais quelques nuances de bleu ne font jamais de mal.

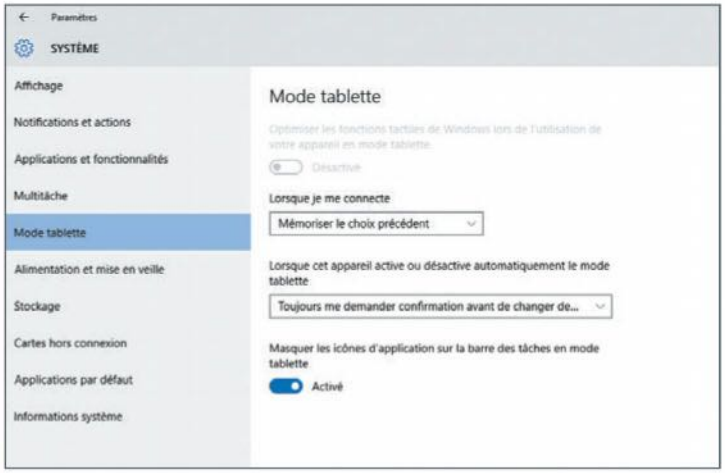


exIT

Modern UI

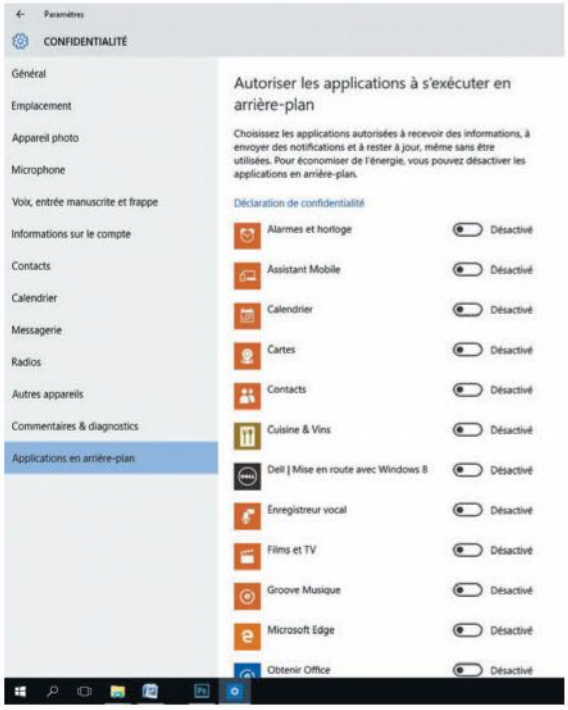
Une interface multisupport

Modern UI a été conspué et reste haï par bon nombre d'utilisateurs de PC. Promis, a tempéré Microsoft, Windows 10 l'enterre (un peu) et revient aux fondamentaux avec le célèbre menu Démarrer. Toutefois, les tuiles n'ont pas totalement disparues : on les retrouve dans ledit menu Démarrer, mais aussi dans l'écran d'accueil. Sur ordinateur, celui-ci est désactivé par défaut, mais les propriétaires d'une dalle tactile ou ceux qui s'y étaient habitués le retrouveront avec une simplicité enfantine. Dans l'onglet Personnalisation des Paramètres, la rubrique Accueil comporte une ligne Utiliser le menu Démarrer en plein écran. Il suffit de l'activer pour retrouver l'interface Modern UI. Néanmoins, cet écran n'est pas figé : il est nécessaire de passer par le bouton Démarrer pour l'afficher. Sur une Surface, cette interface est active par défaut, mais Microsoft joue de versatilité avec son nouvel OS. L'interface « switche » vers le bureau classique dès qu'un clavier externe est détecté. En outre, il est possible d'effectuer la transition manuellement, via un bouton placé dans le coin droit de la barre de tâches ou en passant par les Paramètres Systèmes et en activant le Mode tablette. Notons que l'utilisateur peut régler lui-même le changement de mode (automatique ou non, option au lancement…) via cette même page.



Sous le capot

Des performances loin des sommets



Si Windows 10 constitue une nette amélioration par rapport à Windows 7, il n'apporte pas d'importantes augmentations de performances dès lors qu'on le compare à Windows 8.1, quel que soit le média exécuté. En attendant Direct X12, il ne faut pas espérer jouer au dernier jeu vidéo à la mode en 4K à 60 fps sur une machine de milieu de gamme. Sous Windows 8.1, un certain nombre de processus Windows s'exécutaient en permanence, réduisant les performances d'un ordinateur, parfois de moitié. Après vérification sur plusieurs machines, la migration vers Windows 10 n'a pas résolu le problème, les processus n'ont pas bougé d'un pouce, monopolisant 30 à 50 % de la RAM. Notons cependant que Microsoft a rationalisé les autorisations des applications à s'exécuter en arrière-plan. Elles sont regroupées dans Paramètres>Confidentialité>Applications en arrière-plan. Désactiver leur exécution permet non seulement de gagner quelques Mégaoctets, mais aussi d'économiser la batterie sur les portables et d'éviter que certains programmes collectent impunément vos données personnelles.

Windows Update

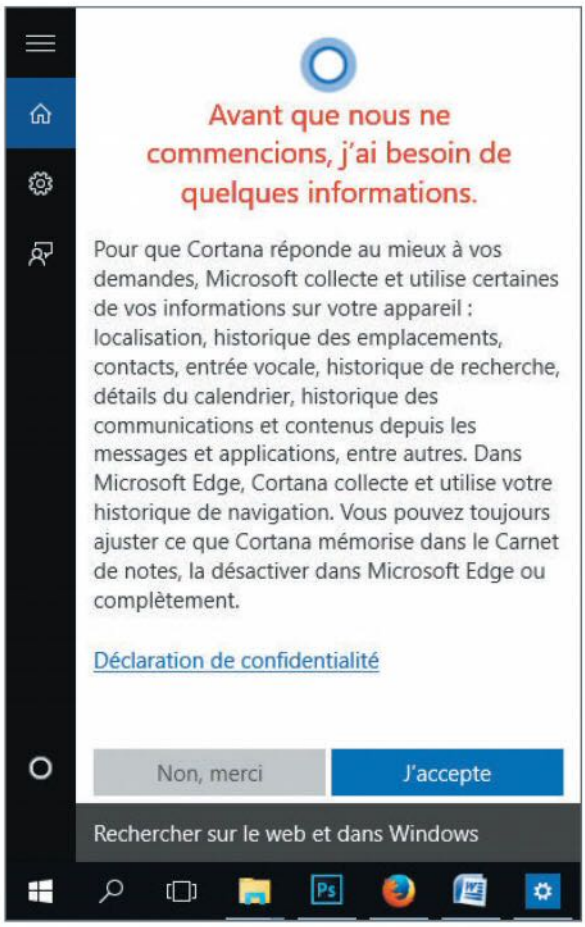
Des mises à jour à votre rythme

Alors que nous écrivons ces lignes, Windows 10 a connu déjà pas moins de trois mises à jour. Et, à chaque fois, un redémarrage automatique est obligatoire. Ainsi, ce malotru est susceptible de vous interrompre en plein travail en exigeant que vous laissiez tout en plan pour le relancer. C'était sans compter sur le nouvel outil de planification des redémarrages. Lequel se situe dans Paramètres>Mise à jour et sécurité>Windows Update>Options avancées. Là, vous aurez tout loisir de demander à Windows 10 de vous *« informer de planifier un redémarrage »* plutôt que de le laisser automatiser le processus. Alors, si une mise à jour est en attente, vous pourrez, via le centre de notifications, décider de l'horaire qui vous convient.

Autre nouveauté à utiliser, les Fast & Slow Rings. Si elles ne sont pas décrites de la sorte dans la version française du système d'exploitation de Redmond, ces deux options vous autorisent à choisir la fréquence des mises à jour, en les reportant – ce qui n'affecte pas les mises à jour de sécurité – ou en obtenant les « builds Insider ». Avec ce dernier, vous aurez, avant tout le monde, les mises à niveau de l'OS, à vos risques et périls en cas de problème de stabilité et/ou de sécurité.

Assistante vocale virtuelle

Cortana, votre secrétaire, se révèle intrusive



Soyons franc : Cortana, à l'instar de Siri, est un outil formidable. Imaginez : une assistante vocale qui répond à toutes vos questions, en exploitant Internet ou vos données locales. « Dis moi Cortana » et votre assistante s'active, avec, si vous le souhaitez, une option de reconnaissance vocale empêchant un tiers de pouvoir la commander. Météo, cours de la Bourse, recherche web, ouverture d'un programme… Cortana acceptera même vous chanter une berceuse.

Sauf que cette chère Cortana a besoin, pour être efficace, de tout connaître de vous. Au lancement, elle vous demande en effet de vous identifier à l'aide d'un pseudonyme – étape qu'il est possible d'ignorer. Ce n'est pas le cas de votre géolocalisation, obligatoire ; ni de la connexion avec un compte Microsoft, également nécessaire. Et vous aurez à accepter ses conditions générales d'utilisation. Dès lors, Cortana aura accès à vos contacts, votre calendrier, vos mails, votre historique de navigation, vos fichiers. Tout…

Si vous craignez pour votre vie privée, une solution radicale s'impose : désactiver Cortana ! Ce qui ne demande guère d'effort : cliquez sur l'engrenage à gauche de l'écran dans le champ de recherche et décochez Activer Cortana. Vous voilà débarrassé de l'intrusive. Si vous souhaitez conserver son assistance vocale tout en protégeant au mieux vos données, il existe des alternatives. En premier lieu, désactivez la géolocalisation. Ensuite, dans Paramètres>Confidentialité, décochez l'autorisation de Cortana d'utiliser vos applications (Contacts, Calendrier, Messagerie…). Enfin, supprimez les informations contenues dans le Cloud, liées à votre compte Microsoft. En limitant ainsi Cortana dans ses mouvements, elle sera bien sûr moins pertinente dans ses réponses. Il vous faudra donc trouver un juste milieu entre protection de la vie privée et confort d'utilisation : une nécessité sous Windows 10.

Navigateur web

Edge : des fonctionnalités gadget ou productives ?

Dans la famille des navigateurs, Edge (ex-Spartan) fait figure de petit dernier. Pourtant, d'après certains benchmarks il égalise déjà ses aînés, voire les surpasse selon d'autres. Annotation de site, possibilité de sauvegarde et de partage. En dépit du profond desamour que nous pouvions vouer à son prédécesseur, Internet Explorer, force est de reconnaître que Edge a de quoi séduire. Plus que ses performances, ses fonctionnalités sont sa véritable valeur ajoutée. Par exemple, le fait d'épingler une page web à l'écran d'accueil n'est pas sans évoquer la conversion, sur mobile, de Favoris en icônes. Soit des liens rapides, plus accessibles encore qu'une simple barre de favoris.

Notons aussi l'outil permettant d'annoter une page web. Alors oui, ça sonne très « gadget » et Microsoft n'arrange rien avec ses publicités où de sympathiques mais écervelés internautes s'amusent à taguer les photos de leurs amis sur Facebook… Pourtant, on peut lui trouver bien d'autres usages, y compris dans un cadre professionnel. Il faut rappeler qu'une Note web peut être enregistrée en Favori mais aussi partagée par mail ou OneNote. Tracer un itinéraire pour votre prochaine randonnée pédestre sur une carte, envoyée par courrier électronique à vos compagnons de route, lesquels la modifient à leur tour… C'est certes moins pratique que MyMaps de Google, mais beaucoup plus intuitif. De même, la page web devient un véritable plan de travail, découpée, commentée, surlignée… Un bon point pour le navigateur de Microsoft, nouvel ami des blogueurs sans-le-sou en quête de feedbacks.

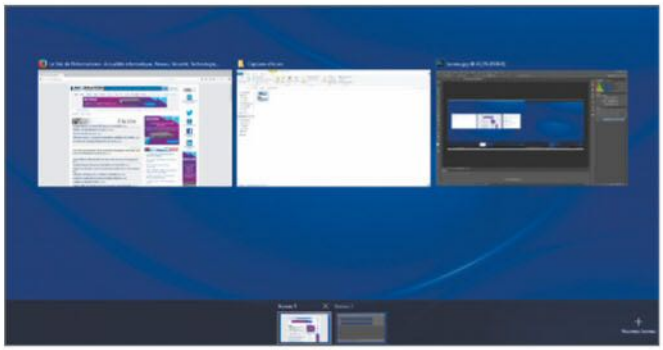
Programmes

Gestion des applications

On se rappellera, dans le Panneau de configuration, la fonction Modifier/Désinstaller des programmes. Windows 10 reprend le système en l'améliorant. Dans l'onglet Système, on trouve tout d'abord la rubrique Applications et fonctionnalités, qui classe les différents programmes installés sur une machine. Le tri se fait par taille, nom de fichier ou encore date d'installation et se paie même le luxe d'avoir un moteur de recherche permettant de trouver plus aisément une application, avant de la désinstaller ou de la déplacer. C'est d'ailleurs via cette page qu'il est possible de paramétrer les « fonctionnalités facultatives » à savoir ajouter des langues de saisie et de synthèse vocale – pour Cortana. Ensuite viennent les Applications par défaut, le fameux *« Avec quelle application souhaitez-vous ouvrir ce fichier? »*. Avec Windows 10, tout y est centralisé, un atout comparé aux versions précédentes. En deux clics, l'utilisateur définit son lecteur vidéo ou musical, son navigateur web ou encore sa messagerie électronique par défaut. Ce mécanisme va un peu plus loin puisqu'il offre la possibilité de définir des applications par défaut par type de fichier, par protocole ou par valeur.

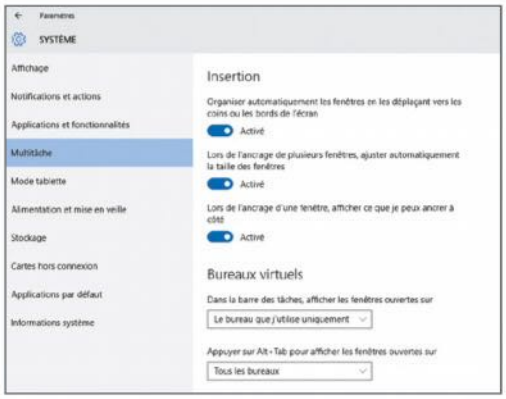
Multitâche

Bureaux virtuels à volonté



Les bureaux virtuels sont bien connus des utilisateurs de Mac, beaucoup moins de la part des Pécéïstes. Windows 10 y remédie en permettant de créer plusieurs espaces de travail dans une même session. Par exemple, vous pourrez disposer d'un bureau virtuel pour le travail, l'actu, les applications productivité… et un autre pour le divertissement. Très pratique dans un environnement professionnel ! Créer, visualiser et changer de bureau est simple comme bonjour. Ainsi, passer une application d'un bureau à l'autre se fait par glisser-déposer. Notez la présence de l'icône à droite du champ de recherche. Elle ouvre un menu donnant accès aux différents bureaux, aux fenêtres ouvertes dans l'espace pour sélectionner un bureau, passer de l'un à l'autre, en créer un nouveau ou en supprimer… C'est sans doute le nouvel outil le plus utile sur le petit dernier de Microsoft.

Le multitâche occupe donc une place de premier ordre dans Windows 10. On déplorera uniquement l'absence de fenêtre pop-up demandant de confirmer la fermeture d'un bureau virtuel. Prudence, mieux vaut ne pas être atteint d'une frénésie de clics. Les utilisateurs confirmés que vous êtes exploiteront probablement les raccourcis clavier pour optimiser la productivité. Voici donc une liste des principaux raccourcis destinés à l'utilisation des bureaux virtuels :



- [Windows] + [Tab] affiche tous les bureaux créés,
- [Alt] + [Tab] affiche les applications ouvertes sur l'appareil
- [Windows] + [CTRL] + [D] ajoute un bureau virtuel
- [Windows] + [CTRL] + [flèches gauche/droite] bascule d'un bureau à l'autre

Enfin, le multitâche est paramétrable, via (à nouveau) Paramètres>Système. Vous pourrez y définir l'affichage des applications et fenêtres sur la barre des tâches pour tous les bureaux ou seulement celui utilisé, ou encore la visualisation des fenêtres via [Alt] + [Tab]. La page Multitâche ne consiste pas uniquement en des bureaux virtuels : l'organisation et l'ancrage des fenêtres ouvertes s'y paramètrent également. ✖

GUILLAUME PÉRISSAT

L'INFORMATICIEN

RÉDACTION
3 rue Curie, 92150 Suresnes – France
Tél. : +33 (0)1 74 70 16 30
Fax : +33 (0)1 41 38 29 75
contact@linformaticien.fr

DIRECTEUR DE LA RÉDACTION : Stéphane Larcher

RÉDACTEUR EN CHEF : Bertrand Garé

RÉDACTEUR EN CHEF ADJOINT : Émilien Ercolani

RÉDACTION DE CE NUMÉRO :
Sophy Caulier, François Cointe, Nathalie Hamou, Loïc Duval, Guillaume Périssat, Yann Serra, Thierry Thaureaux

SECRÉTAIRE DE RÉDACTION : Jean-Marc Denis

CHEF DE STUDIO : Franck Soulier

MAQUETTE : Aurore Guerguerian

PUBLICITÉ
Benoît Gagnaire
Tél. : +33 (0)1 74 70 16 30
pub@linformaticien.fr

ABONNEMENTS
FRANCE : 1 an, 11 numéros,
47 euros (MAG + WEB) ou 42 euros (MAG seul)
Voir bulletin d'abonnement en page 76.
ÉTRANGER : nous consulter
abonnements@linformaticien.fr
Pour toute commande d'abonnement d'entreprise ou d'administration avec règlement par mandat administratif, adressez votre bon de commande à :
L'Informaticien, service abonnements,
28 rue Jean Jaurès 92800 Puteaux - France
ou à abonnements@linformaticien.com

DIFFUSION AU NUMÉRO
Presstalis, Service des ventes :
Pagure Presse (01 44 69 82 82,
numéro réservé aux diffuseurs de presse)
Le site www.linformaticien.com
est hébergé par ASP Serveur

IMPRESSION
LÉONCE DESPREZ (62)
N° commission paritaire : en cours de renouvellement
ISSN : 1637-5491
Dépôt légal : 3e trimestre 2015
Ce numéro comporte pour l'édition abonnés : un encart d'invitation salon Solutions ERP, un encart d'invitation salon Mobility for Business ainsi qu'un cahier spécial Microsoft Visual Studio de 32 pages.

DIRECTEUR DE LA PUBLICATION : Stéphane Larcher

L'INFORMATICIEN est publié par la société L'Informaticien S.A.R.L. au capital de 180310 euros, 443 401 435 RCS Versailles.
Principal associé : PC Presse, 13 rue de Fourqueux 78100 Saint-Germain-en-Laye, France

Un magazine du groupe PCpresse,
S. A. au capital de 130000 euros.

DIRECTEUR GÉNÉRAL : Michel Barreau

les assises

de la sécurité et des systèmes d'information

L'ORIGINAL

15e ÉDITION

L'ÉVÉNEMENT JAMAIS ÉGALÉ

Du 30 septembre
au 3 octobre 2015

MONACO

www.lesassisesdelasecurite.com

LinkedIn YouTube

un événement
COMEXPOSIUM
The place to be

DC consultants

www.infoflash.fr

.NEXT ON TOUR

100 Villes. 36 Pays. 1 Vision.

Participez à .NEXT on Tour en France
et retrouvez-vous aux premières loges lorsque
nous dévoilerons Nutanix Acropolis et Prism.

La plateforme Nutanix XCP

1. Rend l'infrastructure invisible pour les applications d'entreprise.
2. Simplifie le datacenter avec une solution hyper-convergée.
3. Apporte une prédictibilité de la performance et des coûts.

Nutanix Acropolis comprend les services de stockage distribués, les services de mobilité applicative multi-noeuds, multi-hyperviseurs et à terme, multi-cloud (privé ou public) ainsi qu'un hyperviseur embarqué.

Nutanix Prism est l'interface de gestion distribuée de Nutanix qui permet de gérer son infrastructure virtuelle en mode "one click", le plus simplement possible.

Trouvez votre ville : nutanix.com/nexttour

LYON
Mardi 29 septembre 2015

PARIS
Jeudi 8 octobre 2015

NANTES
Jeudi 1er octobre 2015

MARSEILLE
Jeudi 15 octobre 2015

NUTANIX™