N° 126 - Juin 2013 - www.ITPro.fr

IT Pro Magazine®

Le mensuel informatique pour la gestion et l'optimisation des environnements IT Professionnels

IT-Media

Dossier IT Pro

SPÉCIAL SÉCURITÉ

- Et si on parlait authentification forte ?
- La sécurité des grandes entreprises accessible aux PME
- La sécurité d'Android en question
- Le signalement tardif des terminaux perdus

Dell recommande Windows.

Le pouvoir d'en faire plus

Dell : accompagnateur de projets.

Tablette Latitude 10

La productivité complète d'un PC dans la nouvelle tablette tactile Latitude 10 équipée de Windows 8 et d'options de stations d'accueil flexibles.

À partir de

479 €HT

Livraison gratuite

Processeur Intel® Atom™ Z2760
En option, 3 ans de service Pro Support avec intervention sur site le jour ouvré suivant

Serveur PowerEdge T320

Des serveurs dédiés aux entreprises ayant jusqu'à 75 employés, faisant de la communication et la collaboration une priorité.

Économisez 1 161 €HT

1 299 €HT Avant 2 460 €HT

Processeur Intel® Xeon® E5-2403 inclus.
Inclus 3 ans de service Pro Support avec intervention sur site le jour ouvré suivant

Ultrabook™ Latitude 6430u

Conçu pour les entreprises, doté de la technologie vPro pour vous offrir des niveaux de productivité optimisés par les processeurs Intel® Core™ de 3e génération.

Économisez 269 €HT

899 €HT Avant 1 168 €HT

Livraison gratuite

Processeur Intel® Core™ i3-3217U inclus.
En option, 3 ans de service Pro Support avec intervention sur site le jour ouvré suivant

Dell propose aux professionnels :

- Des experts directement à votre écoute 7j/7
- Facilités de financement et de crédit
- L'installation de votre matériel
- Service "Next Business Day" : intervention sur site le jour ouvré suivant
- Assistance matérielle multi-marques
- Offre de reprise de votre ancien matériel : Recyclez et économisez jusqu'à 300 €(1)

Offres valables jusqu'au 14/06/2013, sauf mention contraire.

Visitez Dell.fr/pme ou appelez 0 825 889 885

Du lundi au vendredi de 9h à 19h. Numéro Indigo : 0.15 €TTC/min.

intel inside™ CORE™ i3

IT Pro Magazine

Le mensuel informatique pour la gestion et l'optimisation des environnements IT Professionnels

Un mensuel informatique professionnel édité par IT Media.

Directeur de la Publication : Sabine Terrey.
IT Media – BP 40002 – 78104 St Germain en Laye Cedex – France
Tél. 33 1 39 04 25 00 – Fax. 33 1 39 04 25 05 – www.iTPro.fr

Rédaction

Directrice de la rédaction
Sabine Terrey – sterrey@itpro.fr
Tél. 01 39 04 24 85 – Fax . 01 39 04 25 06

Comité de Rédaction de ce numéro
Sabine Terrey, Wieland Alge, Emmanuel Le Bohec, Guillaume Rameaux, Cyrille Badeau, Jean-Noël de Galzain, Benoit Micaud, Denis Gadonnet, Jean-Claude Bellando, Rich Makris, Emmanuel Macé, Nabil Babaci, Arnaud Alcabez, Loïc Thobois, Eudes-Olivier Robert, Olivier Gerling, Cécile Coste, Laurent Teruin, Arezki Hamadi, Olivier Mendes.

Direction artistique
Célia Schwab

Gestion – Finance

Directeur des opérations
Renaud Rosset – rrosset@itpro.fr
Tél. 01 39 04 24 80 – Fax. 01 39 04 25 05

Responsable financière
Stéphanie Delhaye – sdelhaye@itpro.fr
Tél. 01 39 04 24 82 – Fax. 01 39 04 25 05

Publicité – Marketing

Directeur commercial
Christophe Rosset – crosset@itpro.fr
Tél. 01 39 04 24 95 – Fax. 01 39 04 25 05

Responsable commerciale
Myriam Ifrah – mifrah@itpro.fr
Tél. 01 39 04 24 94 – Fax. 01 39 04 25 05

Responsable commerciale
Emilie Vard – evard@itpro.fr
Tél. 01 39 04 24 91 – Fax. 01 39 04 25 05

Responsable conseil
Karine Latos-Maina – klatos@itpro.fr
Tél. 01 39 04 24 92

Webmaster éditorial
Guillaume Rameaux – grameaux@itpro.fr
Tél. 01 39 04 24 84 – Fax. 01 39 04 25 05

Conception & Réalisation
Agence Com4Medias – www.com4medias.com

Services abonnements & diffusion
Myriam Ifrah – abonnement@itpro.fr
www.itpro.fr/contact-service-abonnement
Tél. 01 39 04 24 94 – Fax. 01 39 04 25 05

Imprimé en France par
IDSL
87400 St Léonard de Noblat

Diffusé en France par
INFO Routage
87000 Limoges

Dépôt légal : À parution
N° ISSN 1961-3814

Site officiel : www.iTPro.fr

Sécurité au quotidien !

Cher abonné, cher lecteur, cher professionnel des environnements Windows Server

Les beaux jours arrivent et les bonnes résolutions « sécuritaires » au sein des organisations se poursuivent ! Une nouvelle ère est déjà bien amorcée, la sécurité de l'information, des applications et des données critiques est en jeu.

Entre authentification et protection des accès informatiques, savoir doser pour conserver le juste équilibre est une des priorités évidentes. Analyse et prudence sont de bons conseils, surtout lorsqu'on s'égare, à juste titre, du côté des nouveaux réseaux de communication… Face à l'évolution des menaces, au volume et à l'émergence de nouvelles attaques, les systèmes traditionnels de défense ne sont plus à la hauteur et semblent désuets, s'armer et s'équiper au mieux devient le défi quotidien des équipes IT.

D'une stratégie de sécurité cohérente à la prise de conscience des nouveaux dangers et besoins, des échanges numériques à la gouvernance des flux, des grandes entreprises aux PME, les vulnérabilités et les réseaux sont très différents. Adapter la sécurité des systèmes d'information est à portée de main mais cette approche passe d'abord par la compréhension de chaque infrastructure et des services qui l'entourent. Alors, tous à vos projets de sécurité ! D'une architecture aux bases solides, il n'y a qu'un pas pour accélérer le business et la compétitivité de l'entreprise…

Nous vous souhaitons une riche et estivale lecture !

Bien cordialement

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

IT Pro Magazine

IT Media - Service des abonnements
BP 40002 - 78104 St Germain-en-Laye Cedex - France
Tél. 01 39 04 25 00 - Fax. 01 39 04 25 05
abonnement@itpro.fr - 1 an soit 10 n° : 95 € TTC

IT Pro Magazine fédère et accompagne la communauté des responsables informatiques d'entreprise en charge de la gestion et de l'optimisation des environnements IT Professionnels, environnement réseaux et serveurs, environnement de bases de données et applicatifs. Toute la richesse des publications IT Media réside dans la combinaison unique de contenus à la fois technologiques et stratégiques. Plus d'informations sur **www.iTPro.fr**

Sommaire

Dossier IT Pro

Spécial Sécurité

Quelle stratégie de sécurité cohérente adopter ?

Ressources IT

Dossier Sécurité

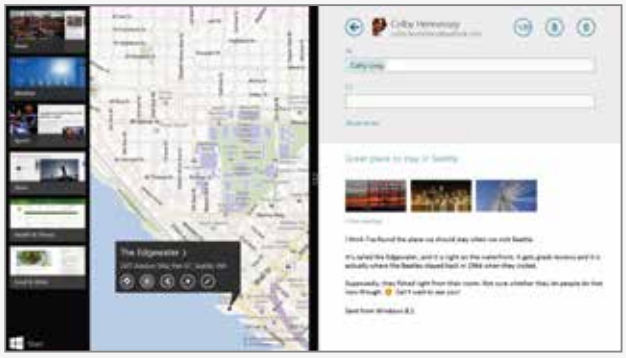
IT Pro Magazine constitue un formidable support pour accompagner vos compétences et vous aider à tirer le meilleur profit de vos environnements informatiques d'entreprise.

Abonnez-vous en page 55 ou connectez-vous sur www.itpro.fr

Nouveau démarrage pour Windows 8

« Nous avons appris de nos clients la façon dont ils utilisent le produit et avons reçu de nombreux retours. Nous ne faisons que commencer et le potentiel est immense. » Antoine Leblond, Vice-Président de Microsoft, a révélé quelques détails supplémentaires sur Windows 8.1, la future version du système d'exploitation. L'éditeur semble avoir pris en compte les critiques adressées à son nouveau système depuis le lancement il y a 7 mois.

Au programme, davantage de personnalisation avec la possibilité d'utiliser le même fond d'écran sur l'écran de démarrage et le bureau classique, amélioration du multitâches avec trois applications affichées simultanément et surtout retour du bouton « démarrer ». Ou du moins d'une fonctionnalité approchante. Microsoft a effectivement inclus un bouton « Start » qui renvoie l'utilisateur vers un écran réunissant l'ensemble des applications. Ces dernières peuvent être triées par date, nom ou catégorie ou fréquence d'utilisation. Il ne s'agira donc pas du menu « démarrer » sous la forme que l'on a connu avec les anciennes versions de Windows. Et malgré des rumeurs insistantes, rien n'a été confirmé quant à la possibilité d'ouvrir sa session directement dans l'interface desktop.



Le bouton « démarrer » fait son retour dans Windows 8.1.

Windows 8.1 sera également livré avec la version 11 d'Internet Explorer. Peu d'informations dévoilées pour l'instant sur le nouveau navigateur, hormis la possibilité d'afficher la barre d'adresse en continu, d'ouvrir autant d'onglets que l'on souhaite et de synchroniser les onglets ouverts avec d'autres terminaux Windows 8.1.

D'autres informations devraient être distillées dans les prochaines semaines, jusqu'à la sortie de la Preview annoncée pour le 26 juin.

Sur iTPro.fr : Windows 8.1 en approche
bit.ly/windows-8-1-approche

Vente de serveurs : Dell se rapproche de HP et IBM

Alors que le marché PC vient de connaître une chute vertigineuse avec des ventes en baisse de 14 % au premier trimestre, l'activité serveur n'est pas non plus au meilleur de sa forme. Sur les trois premiers mois de l'année 2013, les revenus mondiaux générés par la vente de serveurs ont diminué de 5 % par rapport à 2012 selon une étude Gartner.

Si les constructeurs américains IBM et Dell sont toujours en tête du classement (voir le tableau ci-dessous) avec environ 3 milliards de dollars de chiffre d'affaires, c'est leur compatriote Dell qui affiche la plus belle progression. L'entreprise texane est même la seule parmi les cinq principaux vendeurs à connaître une croissance de ses revenus. Alors que les deux leaders enregistrent une baisse de respectivement 13,6 % et 14,4 %, la firme dirigée par Michael Dell réalise un bond de 14,4 % qui lui permet de passer la barre des 2 milliards de dollars de chiffre d'affaires. En termes de parts de marché, Dell passe donc en un an de 14,9 % à 18 % et se rapproche ainsi du duo de tête.

Derrière, Fujitsu et Oracle complètent le top 5 avec un CA en baisse de 6,9 % pour le groupe japonais et 27,2 % pour la société de Larry Ellison.

Sur iTPro.fr : IBM pourrait vendre une part de son activité serveur à Lenovo
bit.ly/ibm-vente-serveur-lenovo

TABLEAU 1 Ventes mondiales de serveurs au premier trimestre 2013 en valeur

Company	1Q13 Revenue	1Q13 MarketShare (%)	1Q12 Revenue	1Q12 Market Share (%)	1Q13-1Q12 Growth (%)
IBM	3,016,060,031	25.5	3,490,477,200	28.0	-13.6
HP	2,959,030,197	25.0	3,455,759,513	27.8	-14.4
Dell	2,124,462,397	18.0	1,857,578,951	14.9	14.4
Fujitsu	583,238,840	4.9	626,721,932	5.0	-6.9
Oracle	538,542,499	4.6	739,825,931	5.9	-27.2
Others	2,604,390,348	22.0	2,273,724,071	18.3	14.5
Total	11,825,724,312	100.0	12,444,087,599	100.0	-5.0

Vers la fin du roaming en Europe ?

Neelie Kroes est particulièrement déterminée. La Commissaire européenne en charge de la société numérique veut en finir avec les frais de roaming au sein de l'Union Européenne. Ces surtaxes sont appliquées par les opérateurs lorsqu'un utilisateur se sert de son terminal à l'étranger pour appeler, envoyer des SMS ou accéder à internet. Le 30 mai dernier, face au Parlement Européen, la responsable néerlandaise a appelé à la création d'un marché unique des télécoms. « Je veux que vous soyez en mesure de vous présenter devant vos électeurs et de leur dire que vous avez réussi à mettre un terme aux frais d'itinérance mobile », a indiqué Neelie Kroes aux parlementaires. Et cette dernière ne souhaite visiblement pas perdre de temps puisqu'elle se dit convaincue que la réforme pourrait être finalisée d'ici mai 2014.

D'ici là, la réglementation concernant les plafonds tarifaires va de nouveau évoluer. Selon le calendrier adopté en mai 2012, le prix maximal facturé pour un mégaoctet de données transféré passera de 70 à 45 centimes à compter du premier juillet 2013. Les baisses concerneront également les appels et SMS (voir tableau ci-dessous). De nouvelles diminutions sont également programmées pour le 1er juillet 2014. A moins que Neelie Kroes n'arrive à tenir son planning.

L'appel de Neelie Kroes à la fin du Roaming a été largement relayé sur Twitter.

Sur iTPro.fr : 150 millions d'euros pour les « filières numériques prioritaires »
bit.ly/filieres-numeriques-prioritaires

TABLEAU 1 Plafonds tarifaires pour le marché de détail (imposés aux consommateurs) hors TVA

	1er juillet 2012	1er juillet 2013	1er juillet 2014
Données (par mégaoctet)	70 centimes	45 centimes	20 centimes
Appels téléphoniques passés (par minute)	29 centimes	24 centimes	19 centimes
Appels téléphoniques reçus (par minute)	8 centimes	7 centimes	5 centimes
SMS (par SMS)	9 centimes	8 centimes	6 centimes

24,2 millions d'abonnés haut débit en France

L'Arcep (Autorité de régulation des communications électroniques et des postes) vient de publier ses derniers chiffres sur le marché du haut et très haut débit fixe en France. Selon son relevé, il y avait au 31 mars 2013 24,2 millions d'abonnés dans l'hexagone, soit une hausse de 260 000 abonnement sur le premier trimestre et de 1,2 million sur un an.

Parmi eux, 22,5 millions (92,98 %) disposent d'un abonnement à haut débit, c'est-à-dire dont le débit maximum descendant est inférieur à 30 Mbit/s. Les 1,7 million d'abonnés restants (7,02 %) sont les quelques chanceux qui bénéficient d'un abonnement à très haut débit en fibre optique. Les réseaux FTTH (fibre optique jusqu'au domcilie) sont encore moins nombreux avec seulement 365 000 abonnements. Si ce chiffre représente donc encore une faible minorité des abonnés à internet (1,51%), la courbe de progression est encourageante puisqu'il a augmenté de près de 70 % en une année.

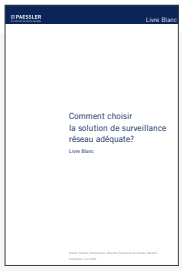
Le 20 février dernier, François Hollande avait dévoilé un programme d'investissement de 20 milliards d'euros pour couvrir 50 % du territoire en très haut débit d'ici cinq ans, et l'intégralité du pays en 2023 (voir *IT Pro Magazine* n°123 – Mars 2013).

Sur iTPro.fr : Vidéo – Akamai : « Internet n'a pas été conçu pour son utilisation actuelle »
bit.ly/internet-utilisation-actuelle

Ressources IT à la une sur ITPRO.FR

Ressources IT exclusives à télécharger sur : www.itpro.fr/r

Le centre de Ressources IT présente un ensemble de ressources éditoriales, unique en téléchargement gratuit. Couvrant la plupart des grands projets d'informatique d'entreprise avec des Hors-Série et des Dossiers exclusifs publiés par la rédaction, des Etudes, des Livres blancs, des Vidéos et des WebCast, mis à votre disposition par nos partenaires.



Comment choisir la solution de surveillance réseau adéquate ?

La surveillance réseau inclue dans la politique informatique de l'entreprise est rentable à plusieurs égards : elle permet des gains de temps considérables, facilite la planification des ressources pour les administrateurs et contribue à optimiser les performances du réseau de l'entreprise… découvrez comment avec ce livre blanc.

■■■■□ | Par Paessler | 12 pages

Accélérez votre business avec SQL Server 2012

Bien plus qu'un SGBD, SQL Server 2012 s'affirme comme une vraie solution complète couvrant tous vos besoins en matière de données, du transactionnel au Big Data, en passant par l'analytique, le décisionnel et l'ETL. Découvrez maintenant comment accélérer concrètement votre business avec SQL Server 2012...

■■■■□ | Par IT Pro Magazine | 4 pages

Comment combattre les attaques DDoS ?

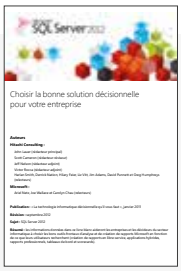
Les attaques de déni de service distribué (DDoS) constituent un risque majeur pour l'entreprise, Téléchargez le Livre Blanc « Attaques de déni de service : Planification des mesures d'atténuation » pour découvrir les mesures préventives et les technologies qui peuvent protéger votre système d'information.

■■■■□ | Par Check Point | 18 pages

Guide de Modernisation des applications IBM i

Vous rêvez d'applications RPG full Web pouvant imprimer et diffuser des fichiers PDF, progressivement accessible depuis des terminaux mobiles ? Vous voulez générer des rapports à partir de requêtes à la base de données et communiquer avec l'extérieur au moyen de Web services ?

■■■■□ | Par PHL Soft Institute | 8 pages



Comment choisir la bonne solution décisionnelle ?

Accompagner les décideurs et responsables IT dans le choix d'outils frontaux d'analyse et de création de rapports en fonction de ce que leurs utilisateurs recherchent - création de rapports en libre-service, applications hybrides, rapports professionnels, tableaux de bord et scorecards...

■■■■□ | Par Microsoft | 32 pages

Découvrez l'imprimante la plus rapide au monde.[1]

Nouvelle HP Officejet Pro Série X. Des impressions deux fois plus rapides et deux fois moins chères qu'avec une imprimante laser.[1,2,3] Grâce à la technologie HP PageWide, l'imprimante multifonction HP Officejet Pro Série X vous permet d'imprimer jusqu'à 70 pages par minute en mode bureautique. Parce que vos clients n'attendent pas. Démonstration sur **hp.com/fr/officejetprox**

Make it matter.*

HP Officejet Pro X

HP PageWide Technology

*Donnez de l'importance

[1]Basé sur les vitesses d'impression les plus rapides établies par les modèles HP X551dw et X576dw, comparées aux performances des imprimantes multifonctions <1000 € et imprimantes laser et jet d'encre couleur <800 € et validées par WirthConsulting.org au mois de janvier 2013. [2]Comparaison basée sur les caractéristiques techniques publiées par les fabricants, sur le mode couleur le plus rapide au mois de mars 2012. Test incluant les imprimantes laser couleur multifonctions <1000 € et les imprimantes laser couleur <800 € disponibles au mois de mars 2012, basé sur la part de marché indiquée par IDC au 1er trimestre 2012 et le test HP réalisé dans le mode couleur le plus rapide. Document test de quatre pages issu d'un fichier certifié ISO 24734. Plus d'informations sur hp.com/fr/ojfacts [3]Coût par page (CPP) établi par rapport à la majorité des imprimantes laser couleur multifonctions <1000 € et imprimantes laser couleur <800 € hors TVA au mois de mars 2012. Pour plus d'informations, rendez-vous sur www.hp.com/fr/officejetprox

Et si on parlait authentification forte ?

Louis Beringer, Directeur commercial Europe du Sud et Patrick Sena, Responsable Avant-Vente, Europe du Sud chez HID Global reviennent sur les problématiques des solutions d'authentification forte et d'identification au cœur des entreprises en mettant en avant diverses approches. Entre savoir-faire sur les moyens d'identification et protection des accès informatiques, le positionnement de ces technologies développées en France répond parfaitement aux besoins actuels.

› Par Sabine Terrey

HID Global propose une approche de l'authentification assez diverse. Des solutions basées sur les cartes à puce aux solutions OTP (One-Time Passeword), les technologies utilisées maîtrisent les moyens d'identification et d'authentification d'un utilisateur sur un réseau d'entreprise (interne, externe, cloud). Face aux besoins des entreprises de plus en plus globaux et multiples, l'identification de l'utilisateur est variable, et peut s'avérer forte en raison de transactions sensibles (secteur bancaire, propriété intellectuelle, accès distant des clients…).

Pour aller plus loin sur ITPro.fr

Dossier Authentification
www.itpro.fr/t/authentification

L'authentification forte en environnement Windows
bit.ly/authentification-forte-windows

ESET® SECURE AUTHENTICATION

VOTRE MOBILE DEVIENT LA CLÉ DE VOTRE SÉCURITÉ

Authentification forte par mot de passe unique
Protège les accès distants contre la faiblesse des mots de passe statiques

- ✓ Protection contre les accès non autorisés
- ✓ Sécurisation des accès VPN et Microsoft® Outlook Web Access
- ✓ Application intégrée à l'Active Directory
- ✓ Aucun matériel supplémentaire requis
- ✓ Mot de passe délivré par SMS ou depuis l'application mobile

TESTEZ GRATUITEMENT PENDANT 90 JOURS

AV comparatives
Record de récompenses Advanced+ lors des tests rétrospectifs AV-Comparatives
www.av-comparatives.org

vb 100 VIRUS virusbtn.com
Record de récompenses VB100 depuis la création de l'organisme en 1998
www.virusbtn.com

www.eset.com/fr

eset®

ENTRE AUTHENTIFICATION ET IDENTIFICATION

Revenons un instant sur ces deux concepts. Si l'identification signifie « dis-moi qui tu es », l'authentification signifie « prouve-le moi ». Plusieurs façons d'authentifier une personne d'ailleurs, l'authentification est dite forte à partir du moment où différents facteurs d'authentification sont impliqués. Les trois facteurs concernent quelque chose qu'on sait et que personne d'autre ne sait, (comme le mot de passe), quelque chose qu'on possède et qui ne peut pas être dupliqué (comme une carte d'identité, un passeport, une carte à puce, un token), et la biométrie (ce qu'on est) à partir des empreintes digitales et rétiniennes.

D'autres facteurs d'authentification alternatifs peuvent entrer en jeu à savoir l'authentification comportementale (navigation sur site internet…), mais ils ne sont pas reconnus aussi sûrement que les trois premiers facteurs classiques.


Louis Beringer

> UNE SOLUTION SÉCURISÉE COMPRENANT L'AUTHENTIFICATION À DEUX FACTEURS AFFINE FORCÉMENT LE POSITIONNEMENT DE L'ENTREPRISE SUR SON MARCHÉ.

Le facteur « ce que je connais », notamment le mot de passe, est le plus répandu, le plus simple et est présent partout aujourd'hui. Cependant, si le mot de passe est volé, il est difficile de s'en rendre compte et on peut assister à une utilisation frauduleuse des comptes par exemple.

Avec le facteur « ce que je possède », face au vol d'un token, il est plus facile de réagir en conséquence. « Le couple le plus communément utilisé est ce que je connais et ce que je possède » explique Patrick Sena. Si le facteur biométrie, ce que je suis, est très prometteur, il n'est pas encore utilisé de manière massive sur les problématiques d'authentification pour des raisons de nécessité de lecteurs biométriques encombrants et onéreux, et d'absence de solutions pragmatiques et simples pour ce facteur d'authentification.

L'AUTHENTIFICATION FORTE EN ENTREPRISE

En entreprise, le facteur « ce que je possède », peut être un certificat qui doit être protégé dans un container (coffre-fort) approprié afin de ne pas être dupliqué. La carte à puce est, aujourd'hui, le meilleur moyen de sécuriser un certificat. L'autre moyen, ce sont les calculettes OTP, tokens qui, à l'aide d'un algorythme pré-défini et d'un secret à l'intérieur de la calculette, vont générer un numéro valable une fois seulement et sur une fenêtre temporelle bien définie. « Ce mot de passe unique, cet OTP, prouve que l'utilisateur possède la calculette associée, et apporte ainsi un deuxième facteur d'authentification » souligne Patrick Sena.

Face à cette approche traditionnelle de l'authentification, le facteur « ce que je possède » est aujourd'hui mutualisé sur quelque chose que l'utilisateur a déjà bien en main, comme un téléphone portable ou un ordinateur.

Il est donc préférable d'agréger au téléphone, par exemple, un moyen d'authentification en utilisant les soft tokens par opposition aux hardware tokens, calculettes physiques. Les soft tokens sont des applications installées sur les téléphones et qui jouent le même rôle que les hard tokens : elles vont générer des mots de passe à usage unique, valables une seule fois, sur un laps de temps défini, et qui vont permettre à l'utilisateur de s'authentifier.

L'authentification forte à destination des clients d'une entreprise (secteur bancaire) peut également être vue et considérée comme rassurante sur le sérieux de son fournisseur. « La perception de l'utilisateur est essentielle : une solution sécurisée comprenant l'authentification à deux facteurs, même si elle semble plus contraignante en termes d'utilisation, affine forcément le positionnement de l'entreprise sur son marché » poursuit Louis Beringer.

L'information est, aujourd'hui ; de plus en plus disponible sous différentes formes et différents moyens, et la mobilité est présente dans toutes les entreprises. Alors, dans ce cas, comment s'assurer que l'information disponible n'est vue et accédée que par les personnes autorisées ? L'accès peut se faire à partir d'une tablette, d'un téléphone ou d'ordinateur portable (astreinte ou home office).

La première préoccupation de l'entreprise est claire :

TRADER'S

Les solutions QUICK-SOFTWARE-LINE

Vous utilisez l'IBM i

Comme serveur de votre base de données

TRADER'S spécialiste du traitement de la donnée IBM i depuis 20 ans
met à votre disposition ses logiciels
pour vous aider à dynamiser vos données

WWW.QUICK-SOFTWARE-LINE.COM

QUICK-EDD/HA
PRA - Haute Disponibilité
Continuité d'activité
24/24 - 7/7

QUICK-EDD/DR
QUICK-EDD/DRm
Réplication - Intégration
et Distribution
(DB2, Oracle, SQL, ...)

QUICK-CSi
Audit - Sécurité
Mise en conformité

QUICK-PRESS
Mise en forme graphique
PCL / PDF / XML

QUICK-DMT
Dématérialisation
et Archivage
à valeur légale

SIMPLE ET PERFORMANT

QUICK-EDD

QUICK-DOC

TRADER'S S.A - 21 Rue Rollin - 75005 Paris - Tél : 01 53 10 27 50 - E-mail : info@traders.fr

le flux de données entre le collaborateur et l'entreprise doit être sécurisé. Il faut donc créer un tunnel VPN (chiffrement de la donnée) mais également se poser la question : qui est au bout de ce tuyau sécurisé ? Pour cela, on intègre un deuxième facteur d'authentification pour que les données transitent vers une personne habilitée à les recevoir.

« Avec les applications de plus en plus disponibles sur Internet et les données de plus en plus situées dans le cloud, l'authentification forte est évidemment primordiale » justifie Patrick Sena. Les entreprises qui se tournent vers les services cloud, ne peuvent se passer de cette authentification forte, afin de couper les accès quand l'entreprise le souhaite.


Patrick Sena

> Si on prend le temps de choisir le moyen d'authentification le plus pertinent pour l'utilisateur, on arrive à quelque chose qui est simple et convivial à utiliser.

QUID DES APPLICATIONS DANS LE CLOUD ?

La plupart des applications dans le cloud propose une solution de délégation d'authentification à savoir la fédération d'identité. Il est possible de s'appuyer sur un tiers de confiance, c'est l'Identity Provider dans le monde de la fédération d'identité, c'est-à-dire en charge de fournir des identités et d'authentifier ces personnes. L'entreprise qui bénéficie de ces services dans le cloud, met en place un Identity Provider en interne, dans son infrastructure informatique, afin de garder la maîtrise de l'authentification même si le service est fourni par un tiers dans le cloud.

Cette approche a donc plusieurs intérêts. D'une part, l'entreprise garde la maîtrise de l'authentification, « les mots de passe sont stockés chez elle » commente Patrick Sena. D'autre part, il est possible de s'appuyer sur des moyens d'authentification déjà en place dans l'entreprise, afin d'éviter la prolifération des mots de passe. Enfin, on peut, avec la fédération d'identité, aussi agréger l'authentification autour de moyens d'authentification mutualisés. Malgré le besoin de sécurité, le confort d'usage reste quelque chose d'essentiel pour l'entreprise, « la volonté est d'avoir des expériences utilisateur le plus uniforme possible quel que soit le moyen d'accéder à l'information » ajoute Patrick Sena.

Les solutions HID Global peuvent ainsi apporter énormément de valeur en faisant de l'authentification forte de manière transparente, et adapter l'ergonomie des applications en fonction du contexte de la connexion. Ce type d'approche répond aux problématiques de BYOD puisqu'on n'interdit à personne d'utiliser un device pour accéder à l'information, par contre, on impose d'avoir un moyen d'authentification adapté au contexte d'utilisation.

L'AUTHENTIFICATION ET LA SÉCURITÉ

La problématique des entreprises est de trouver le bon moyen d'authentification qui permet de répondre à tous les cas d'usage, par l'authentification des employés, des VIP, des fournisseurs, des partenaires commerciaux, des clients.

La solution d'authentification « magique » doit être acceptable d'un point de vue des contraintes d'utilisation et des coûts. Il est indispensable de trouver la solution qui permet d'agréger tous les services d'authentification répondant à ces problématiques. « Cette solution doit être évolutive et souple pour répondre aux problématiques d'aujourd'hui et de demain. Il n'y pas un moyen d'authentification parfait mais une multitude de moyens d'authentification qui utilisés ensemble, fournissent une solution acceptable et à des coûts intéressants pour l'entreprise » admet Patrick Sena.

L'authentification et la sécurité devraient se baser à différentes couches : l'utilisateur ne devrait pas être authentifié de manière périmétrique, une seule fois pour accéder au système d'information, mais l'utilisateur devrait être authentifié au fur et à mesure de son utilisation et de son accès aux données. Plus les données sont sensibles, plus l'authentification devrait être forte.

L'authentification forte peut être très simple à appréhender pour les utilisateurs. « Traditionnellement, son image n'est pas celle du confort d'usage, puisque l'utilisateur est contraint à apporter un secret supplémentaire quand il s'authentifie. Pour autant, si on prend le temps de choisir le moyen d'authentification le plus pertinent pour l'utilisateur, on arrive à quelque chose qui est simple et convivial à utiliser » conclut Patrick Sena. ■

1&1 SERVEUR CLOUD DYNAMIQUE

PUISSANCE FLEXIBLE

PRIX MAÎTRISÉ

à partir de

0,03 €

HT PAR HEURE*

CONTRÔLE TOTAL DES COÛTS

- **NOUVEAU : sans engagement !**
- **NOUVEAU : sans frais de mise en service !**
- **NOUVEAU : sans prix de base !**
- **Durée limitée : jusqu'à 30 € de crédit offert !****
- **Transparence totale** grâce à la facturation horaire à l'usage.
- **Trafic illimité** sans réduction de bande passante.
- **Parallels® Plesk Panel 11 inclus,** noms de domaine illimités.

ACCÈS ROOT COMPLET

- Droits d'administrateur et ressources dédiées pour chaque VM.

HAUTE FLEXIBILITÉ

- vCores, RAM et espace disque configurables séparément : **seulement 0,01 € HT par heure et par unité matérielle !***
- **NOUVEAU : jusqu'à 8 vCores et 32 Go de RAM.**
- Ajoutez jusqu'à 99 machines virtuelles en un seul clic - sans migration !

SÉCURITÉ OPTIMALE

- Disques durs et unités de calcul redondés afin de protéger votre serveur cloud contre toute défaillance.

OPTERON PROCESSOR AMD · SUSE · Parallels Plesk Panel

1&1

MEMBRE DE united internet

DOMAINES | EMAIL | HÉBERGEMENT | E-COMMERCE | SERVEURS

0970 808 911 (appel non surtaxé)

1and1.fr

* Configuration minimale : 1 vCore, 1 Go de RAM et 100 Go d'espace disque, soit 0,03 € HT/heure (0,036 € TTC). Le prix final varie en fonction de la configuration choisie : simulation en ligne sur hosting.1and1.fr/cloud-server-config.

** Crédit de 30 € déduit du montant HT de la 1ère facture, pas de report du crédit non consommé. Détails disponibles sur 1and1.fr.

La prudence est de mise si vous souhaitez garder les données de votre entreprise en toute sécurité

Pour cela, voici quelques astuces sur les différents réseaux de communication.

› Par Wieland Alge

PAR TÉLÉPHONE

Certaines informations sont extrêmement importantes (bancaires ou mots de passe de sécurité), n'utilisez que des sources que vous savez être sûres. Lorsque votre banque vous téléphone pour vous demander des informations spécifiques, ayez en tête que n'importe qui peut se faire passer pour un conseiller et évitez de donner ces informations. Dans ce genre de situation, il est préférable d'être l'auteur du premier contact et ainsi de contacter vous-même votre banque en utilisant les numéros inscrits sur le site et sur les papiers officiels de l'établissement concerné. Même pour les appels des personnes qui déclarent vouloir joindre le patron de votre entreprise, vérifiez systématiquement l'identité de l'appelant avec les protocoles de sécurité de l'entreprise. N'hésitez pas à donner l'alerte si un de vos collègues transgresse les règles que nous venons d'énoncer.

SUR INTERNET

Assurez-vous systématiquement que les URL contenus dans vos emails vous renvoient bien aux bonnes adresses. Malheureusement, de nos jours, les pièges se multiplient de plus en plus. Par exemple, les emails provenant de Paypal ou d'organismes similaires doivent être ignorés. Même si cela prend un tout petit peu plus de temps, nous vous conseillons de taper manuellement l'URL dans votre navigateur puis de vous connecter à votre compte. A partir de là, vous pourrez consulter vos informations en toute sécurité. Si vous répondez à des emails inhabituels, revérifiez toujours le contenu de votre email et de votre liste de destinataires CC. Ayez conscience que, comme la nature humaine, la technologie a toujours des limites. Même avec des programmes adéquats, la sécurité peut être à la merci de l'utilisateur. Une fois ce point compris, cela pourra vous aider à prévenir les attaques.


Wieland Alge

› Si vous répondez à des emails inhabituels, revérifiez toujours le contenu de votre email et de votre liste de destinataires CC.

EN PERSONNE

A l'instar du téléphone, méfiez-vous des personnes qui s'intéressent trop à votre entreprise lors d'une rencontre inopinée dans un café ou lors d'un cocktail. Ce ne sont probablement que des commerciaux mais certains escrocs profitent aussi de ces rencontres. En règle générale, éviter ces deux types de personnes ne vous fera pas perdre grand-chose. Pour les zones sensibles, n'hésitez pas à garder une trace des rapports d'entrée et de sortie. En effet, même une personne haut placée dans la hiérarchie de l'entreprise peut transgresser les règles. Demandez, régulièrement, à tous les employés, nouveaux comme anciens, de présenter un badge lorsqu'ils souhaitent accéder à une zone sensible ou à des données importantes. Nous vous conseillons fortement de former vos employés afin qu'ils aient les connaissances appropriées en matière de sécurité et qu'ils se sentent responsables des données utilisées. Les badges sont aussi importants pour vos visiteurs. N'hésitez pas à fabriquer quelques badges d'identité temporaires et à raccompagnez vos visiteurs à chaque fois. L'art de manier le bâton n'est pas toujours efficace. Félicitez donc publiquement ceux qui signalent les problèmes éventuels et qui prennent des mesures pour les corriger. Si possible, prenez soin de les récompenser. ■

Wieland Alge
Vice-président Europe
Barracuda Networks

Pour aller plus loin sur ITPro.fr

La sécurité SQL contre le vol de données
bit.ly/securite-sql-vol-donnees

La sécurité rétroactive face à la fuite de données
bit.ly/securite-retroactive-fuite-donnees

RAZ-LEE™
Experts @ Security and Compliance

iSecurity

Ayez l'esprit libre grâce à i Security

N°1 mondial des progiciels de sécurité, de contrôle et de conformité d'audit, destinés au système IBM i

- ☑ Couvre l'ensemble des besoins de sécurité de votre Entreprise: intrusions, malveillances...
- ☑ Idéal pour les Auditeurs et les Managers
- ☑ Contrôle les normes PCI, SOX, HIPAA, Bâle II..., ainsi que vos normes spécifiques
- ☑ Très haut niveau de performance
- ☑ Système intégré, modulaire et évolutif pour toute entreprise
- ☑ S'intègre et complète avantageusement une solution existante

Notre site: www.razlee.fr email: andre.meyer@razlee.com

Démystifier les attaques par Déni de service (DDoS) pour mieux s'en protéger ?

› Par Emmanuel Le Bohec

Contrairement aux idées reçues, il existe de nombreuses variantes d'attaques par déni de service, distribuées ou non (DoS/DDoS), visant divers protocoles, volumétriques ou pas, réseau ou applicatives, ainsi que des combinaisons de ces variantes. Les motivations sont également variées : jeu ou simple satisfaction narcissique, manifestation virtuelle aux accents plus politiques ou cyber-guerre économique ou militaire. Les entreprises et organisations de toutes tailles utilisant une connexion internet, disposant d'un serveur web ou d'un réseau accessible de l'extérieur sont directement concernées par ce risque. Les objectifs des attaques sont moins nombreux que leurs types ou motivations : bloquer l'accès à un service – pour perturber l'activité de la victime et provoquer des pertes financières immédiates – ou rendre inopérants des équipements (ou services) et/ou créer une diversion pour faciliter une intrusion. Le plus important est de comprendre que les attaques par déni de service, quel que soit leur type, ne sont souvent qu'un volet d'une attaque structurée, visant en réalité à pénétrer sur le réseau de la cible pour voler des informations stratégiques : brevets, données personnelles, financières, etc.

On peut regrouper ces attaques en cinq grandes familles, des plus volumétriques – mais également plus anciennes, moins élaborées – aux moins volumétriques – plus récentes et élaborées. La première est l'envoi massif de requêtes, utilisant une grande bande passante, que les outils traditionnels de défense peuvent repérer, sans toutefois toujours savoir comment ne bloquer qu'elles pour garantir la continuité du service. La deuxième (reflective DoS attack) est similaire mais utilise un serveur de rebond pour attaquer, pendant que la troisième (outbound DDoS attack), utilise une machine compromise au sein même du réseau cible pour lancer un DoS et bloquer tout ou partie du réseau de la victime. Les deux familles d'attaques restantes visent, elles, la couche applicative des serveurs cibles. Ce sont les plus dangereuses car conçues pour s'attaquer aux applications. Parfois spécifiques, elles n'envoient que très peu de données, ne génèrent pas de pic de bande passante (ainsi Apache killer, conçu pour faire tomber un serveur web avec un seul paquet). Masquées au sein des attaques volumétriques, elles sont d'autant plus dangereuses que leur trafic semble conforme.


Emmanuel Le Bohec

› Le Gartner préconise d'ailleurs de déployer des équipements anti-DDoS en local, puis, éventuellement, de compléter avec une offre opérateur ou MSSP.

C'est d'ailleurs pour cela que les systèmes traditionnels de défense, tels que pare-feu et IPS, ne peuvent lutter. Ils n'ont pas été conçus pour cela. Déjà impactés, quasiment systématiquement par les attaques volumétriques, ils ne voient tout simplement pas les attaques applicatives. Le Gartner préconise d'ailleurs de déployer des équipements anti-DDoS en local, puis, éventuellement, de compléter avec une offre opérateur ou MSSP. En effet, seules des solutions dédiées sur le réseau de l'entreprise peuvent parer à l'ensemble des attaques, car elles analysent aussi bien le trafic que son impact sur les applications hébergées. C'est donc directement devant le réseau qu'il faut installer ces équipements adaptés. Ils joueront le rôle de première ligne de défense, en rejetant tout trafic anormal (et uniquement celui-ci), avant qu'il n'accède au réseau, laissant les pare-feu, en particulier les « Next Generation », jouer pleinement leur rôle classique de contrôle des utilisateurs et des applications. ■

Emmanuel Le Bohec
Regional Manager France, BeNeLux, Suisse et Afrique francophone
Corero Network Security

Pour aller plus loin sur ITPro.fr

Les quatre piliers de la sécurité réseau
bit.ly/piliers-securite-reseau

Comment combattre les attaques DDoS ?
www.itpro.fr/r/comment-combattre-attaques-ddos

Simple. Adaptable. Manageable.

Guides de conception de solutions pour un déploiement facile et rapide !

Simple : Nous sommes déterminés à faire en sorte que nos solutions soient les plus simples à installer, configurer et intégrer au sein des systèmes informatiques existants ou des nouvelles constructions. Nous livrons notre solution aussi « prête à installer » que possible (par exemple, l'installation des bandeaux de prises est sans outil et les fonctionnalités de gestion des câbles sont fournis). Avec notre infrastructure facile à configurer, concentrez-vous sur des préoccupations informatiques plus urgentes telles que les menaces sur le réseau.

Configurations pour tout type d'espace informatique !

Adaptable : Nos solutions sont adaptées à n'importe quelle configuration depuis le petit espace informatique jusqu'aux datacenters ! Les baies informatiques compatibles multi-constructeurs, par exemple, sont livrées en différentes profondeurs, hauteurs et largeurs de telle sorte que vous puissiez déployer votre informatique dans n'importe quel espace à votre disposition, du petit environnement informatique ou des espaces de bureau jusqu'aux datacenters.

Surveillez et gérez vos espaces informatiques où que vous soyez !

Manageable : La gestion locale et à distance est simplifiée avec le contrôle de sortie de l'onduleur la surveillance intégrée de l'environnement local et les rapports d'utilisation énergétique. La facilité de gestion sur le réseau et la création de rapports vous aident à prévenir les problèmes informatiques et à les résoudre rapidement lorsqu'ils se produisent, où que vous soyez ! Qui plus est, nos services de maintenance assurent des opérations optimales.

Infrastructure informatique physique facile à déployer

Les guides de solutions facilitent l'identification de vos besoins pour relever les défis d'aujourd'hui. Le cœur de notre système, les baies informatiques compatibles multi-constructeurs et les bandeaux de prises en rack, rendent le déploiement facile. Des composants ajustables, des supports de fixation intégrés aux baies, des pieds de nivellement préinstallés et des accessoires de gestion de câbles pouvant être montés sans outil favorisent une installation simple et rapide.

Business-wise, Future-driven.™

InfraStruxure

Les solutions InfraStruxure™ intégrées incluent tout ce dont vous avez besoin pour le déploiement de votre infrastructure informatique physique : alimentation électrique de secours et distribution électrique, refroidissement, baies et logiciel de gestion. Gamme de solutions adaptables depuis les plus petits espaces informatiques jusqu'aux datacenters multimégawatts.

Conseillez vos clients pour qu'ils puissent tirer le maximum de leur espace informatique !

Téléchargez aujourd'hui l'un de nos 3 meilleurs guides de conception de solutions et tentez de gagner un iPhone 5.

Consultez : www.apc.com/promo **Code de clé :** 34758p
Téléphone : 0 825 012 999

APC™ by Schneider Electric

La sécurité des grandes entreprises accessible aux PME

Si les technologies de sécurité Check Point Software s'adressent traditionnellement aux grandes entreprises avec des appliances à plusieurs centaines de milliers d'euros, la société israélienne souhaite aujourd'hui s'imposer sur le marché des PME et filiales de grands comptes. Elle lance pour cela plusieurs modèles d'appliances beaucoup plus accessibles. Christophe Badot, Directeur Général de Check Point en France, nous explique cette évolution.

› Par Guillaume Rameaux

IT Pro Magazine : Quels sont aujourd'hui les principaux points faibles des entreprises ?
Christophe Badot : Nous réalisons des tests chez nos clients avec le 3D Security Report dont l'objectif est de voir ce qui se passe en réellement dans leurs systèmes d'informations. Nous en avons extrait 900 cas réels qui nous ont révélé quatre principaux éléments : 75 % des entreprises accèdent à des sites malveillants, 63 % sont infectées par des bots, 54 % subissent des fuites de données et 47 % utilisent des outils pour anonymiser l'utilisation des outils informatiques et contourner ainsi les systèmes de sécurité.

Accès à des sites malveillants, fuites de données, contournement des règles de sécurité, est-ce que la première étape pour une plus grande sécurité ne serait pas de sensibiliser les employés aux risques ?
La sensibilisation des utilisateurs est l'élément clé. Un test de sécurité classique consiste à disséminer quelques clés USB dans un parking. Vous verrez que les 2/3 vont être connectées au SI de l'entreprise par les employés qui les ont trouvées. Un autre exemple de problème bien connu est celui de la complétion automatique des adresses dans Outlook qui génère souvent des erreurs de destinataires lors de l'envoi d'un document. L'éducation est fondamentale. Check Point a justement essayé de mettre l'utilisateur au cœur de la politique de sécurité et d'éviter qu'à vouloir trop fermer un système, cela ne devienne un frein au business. Si quelqu'un tente d'accéder à un site malveillant de manière non volon-

Pour aller plus loin sur ITPro.fr

Dossier PME
www.itpro.fr/t/pme

Les petites entreprises en avance sur l'adoption du cloud
bit.ly/petites-entreprises-cloud


Christophe Badot

» Nous nous sommes aperçus que si les grandes entreprises sont les plus ciblées, de plus en plus d'attaques nous sont remontées sur des organisations de taille inférieure.

taire par exemple, ou d'envoyer par mail un fichier qui n'est pas censé sortir de l'entreprise, une alerte va apparaître pour l'avertir d'une situation à risque. L'utilisateur a alors le choix de tenir compte de l'avertissement ou non. Cela permet de sensibiliser les utilisateurs qui, la plupart du temps, ne pensent pas faire quelque chose de mal.

Vous avez lancé des appliances pour filiales de grands groupes et les petites structures. Est-ce que cela veut dire que les bureaux principaux et les grandes entreprises sont aujourd'hui bien équipés en solution de sécurité ou est-ce la menace qui s'est déportée vers les sociétés de taille plus réduite ?

Nous nous sommes aperçus que si les grandes entreprises sont les plus ciblées, de plus en plus d'attaques nous sont remontées sur des organisations de taille inférieure. Les grandes arrivent à un niveau d'équipement qui les rend difficiles à attaquer. Dans une PME, il y a moins de compétences et de ressources dédiées à la sécurité, ce qui en fait des cibles plus faciles. Nous avons parmi nos clients de grands groupes qui ont des structures traditionnelles avec un ou plusieurs datacenters. Historiquement, nous avons les produits et les fonctionnalités pour bien protéger ces sites centraux. La plupart ont toutefois des sites déportés, des structures de plus petite taille, mais qui ont des besoins de protection équivalente. Il devenait nécessaire de protéger ces sites avec un niveau fonctionnel équivalent aux sites principaux. Nous avons donc lancé les trois appliances 1100 sur lesquelles on pourra retrouver l'intégralité des fonctionnalités logicielles disponibles jusqu'à présent sur du matériel moyen ou haut de gamme. Ce sont des produits qui peuvent s'intégrer dans un réseau de plusieurs appliances supervisées via une console unique ou alors se vendre seuls pour une entreprise de quelques dizaines ou centaines d'employés.

Nous aidons également les petites et moyennes entreprises à vérifier la conformité des systèmes de sécurité. Notre fonctionnalité de compliance va automatiquement contrôler une série de points de conformité et les comparer soit à une politique interne, soit à une norme en vigueur, comme ISO 270001, qui aura été pré-chargée.

Ces appliances ont aussi l'avantage d'être plus accessibles financièrement. Est-ce que la sécurité informatique représente une part importante du budget des entreprises ?

La sécurité a toujours été le parent pauvre. Les entreprises sont prêtes à mettre de l'argent dans un système de production, de comptabilité ou un ERP car elles en voient tout de suite l'apport. Mais il y a une prise de conscience importante du risque de perte de données ou d'indisponibilité du SI. Les attaques touchant le grand public accentuent cette prise de conscience. Aujourd'hui, on parle de phishing au journal de 20 h. Nous sommes donc dans un environnement très hostile et cela aide à faire progresser l'idée que la sécurité est un élément pour lequel l'ensemble des entreprises, de petite, moyenne ou grande taille, doit investir un peu plus d'argent. Mais il faut pour cela proposer une gamme de produits cohérente avec la taille de l'entreprise.

Historiquement, le positionnement de Check Point était plutôt tourné vers les entreprises du CAC 40. Nous continuons à proposer des produits pour ces clients avec des équipements haut de gamme comme le 61 000 qui coûte aux alentours de 500 000 euros mais notre stratégie aujourd'hui est vraiment de pouvoir adresser n'importe quelle taille d'entreprise.

C'est la raison d'être de ces appliances 1 100 avec un point d'entrée à moins de 600 dollars et un prix qui peut monter selon le nombre d'utilisateurs, la configuration matérielle et les fonctionnalités voulues, jusqu'à 2 000 dollars. Cela veut dire qu'on peut avoir une sécurité de qualité et abordable à 400 euros. Nous avons également annoncé, récemment, un nouveau produit à destination des entreprises de moins de 100 salariés, à un prix encore inférieur : l'appliance 600. Le point d'entrée est à 400 dollars. Il s'agit d'une appliance avec toutes les fonctionnalités standard : IPS, filtrage d'URL, VPN, antivirus, antispam, firewall.

Check Point a également annoncé récemment une nouvelle fonctionnalité baptisée Threat Emulation. De quoi s'agit-il exactement ?

C'est une fonctionnalité complémentaire que l'on peut installer sur l'ensemble de nos appliances. Quand un fichier contient une menace encore inconnue, les filtres IPS ou les signatures antivirales ne peuvent la reconnaître. Le principe est donc d'ouvrir le fichier dans une sandbox où on peut observer son comportement en toute sécurité. Si tout est normal, la solution le laisse passer, sinon elle le bloque. Cette simulation d'ouverture est le seul moyen de lutter contre une attaque 0-day. ■

Sécurité adaptative : juste du bon sens !

La plupart des grandes sociétés qui ont été attaquées très sérieusement lors des deux dernières années étaient protégées par des outils de prévention d'intrusions (IPS) sérieux et robustes. Pire encore, les éditeurs d'IPS avaient, dans la quasi totalité des cas, déjà publié une règle de protection pour stopper l'exploit dont elles ont été victimes… Seulement, la règle de protection n'était pas activée au bon endroit et au bon moment.

› Par Cyrille Badeau

L'ARBRE QUI CACHE LA FORÊT

Depuis toujours, les éditeurs ont pointé du doigt et cristallisé notre attention sur la menace et son évolution constante. Les Hackers vont vite, très vite. Il faut donc que les éditeurs fassent d'énormes efforts pour suivre la menace qui est en perpétuel mouvement. Nous le savons tous, un anti-virus ou un IPS qui ne sont pas mis à jour ne servent pas à grand chose… nous mettons donc à jour quasiment quotidiennement. Seulement, dans 90 % des cas, la politique mise à jour est la politique par défaut du constructeur…

POLITIQUE PAR DÉFAUT

Définition : une politique par défaut est une politique créée pour fonctionner sans effets de bord (faux positif) chez tout le monde mais qui ne fait finalement de la sécurité chez personne.

Il est important de noter qu'un « faux positif » n'est pas généré par une règle mal écrite – il est généré par une règle utilisée dans un contexte inapproprié (par exemple, l'activation de règles Apache sera potentiellement génératrice de « faux positifs » si elle est réalisée dans un environnement qui utilise exclusivement des serveurs web IIS).

Afin d'éviter de rejeter du trafic licite, les constructeurs d'IPS proposent donc tous une politique par défaut « garantie » sans faux positifs. Elle s'applique aux systèmes et services les plus courants et les plus utilisés (le plus grand dénominateur commun de nos réseaux). En effet, le risque de faux positif étant fort dans un contexte inadapté, il s'agit de normaliser la politique autour d'un pseudo contexte commun.


Cyrille Badeau

› Il faut réaliser une personnalisation précise pour garantir une protection complète en fonction des vulnérabilités présentes.

Cette politique contient généralement entre 1 000 et 3 000 règles. Pourtant, il existe aujourd'hui plus de 25 000 règles IDS/IPS différentes.

NOS RÉSEAUX SONT TOUS DIFFÉRENTS

Même si nos serveurs de fichiers, nos infrastructures et nos stations de travail sont peu différents d'un réseau à l'autre, nos applications métiers sont clairement toutes différentes en fonction de nos secteurs d'activité mais ont un point commun : elles correspondent au plus fort besoin de sécurisation dans l'entreprise – elles sont nos ressources critiques.

Les politiques par défaut ne sont clairement pas adaptées pour gérer le risque lié à ces ressources critiques. Il faut réaliser une personnalisation précise pour garantir une

Pour aller plus loin sur ITPro.fr

Systèmes de détection des intrusions
bit.ly/systemes-detection-intrusion

Le cryptage des données sensibles au sein des entreprises
bit.ly/cryptage-donnees-entreprise

protection complète en fonction des vulnérabilités présentes.

LE CHANGEMENT C'EST MAINTENANT

Supposons que nous ayons réalisé ce « tuning » précis nécessaire pour réellement tirer un bénéfice de l'outil de sécurité qui protège nos environnements critiques. Nous sommes alors pour quelques heures en mesure de gérer et de contrôler le risque sur cette zone, et ce jusqu'à ce qu'un changement intervienne dans le réseau (nouveau service, nouvelle version, démarrage de machine virtuelle, nouvelles vulnérabilités découvertes).

Dans le réseau d'une grande entreprise, ce changement intervient quasi quotidiennement. Il faut dont « tuner » continuellement pour conserver un niveau de sécurité acceptable. Impossible…

Tous les éditeurs insistent sur les mises à jour nécessaires pour se protéger contre les nouvelles menaces extérieures… Qu'en est-il des changements à l'intérieur du réseau ?

Il est aujourd'hui admis par les spécialistes du domaine que sans adaptabilité ou « tuning » régulier, la protection d'un IPS contre des attaques ciblées est quasi nulle.

SÉCURITÉ ADAPTATIVE OU NGIPS

Ainsi, la sécurité doit être adaptative. Un IPS adaptatif (qui intègre des modules intelligents de découverte du réseau protégé), permet d'avoir une connaissance des OS/Services/Applications/utilisateurs à protéger et ainsi connaître les vulnérabilités potentielles présentes sur les machines tout en sélectionnant pour vous les règles qui doivent être appliquées dans votre environnement et ce dans une base de 25 000 règles disponibles.

Chaque entreprise doit disposer d'une politique IPS spécifique à son environnement, garantissant une protection exhaustive et limitant donc le taux de « faux positifs » au minimum possible.

Dans ce cadre, si une règle doit être déployée devant vos ressources à protéger, elle le sera. ■

Cyrille Badeau
Directeur Europe du Sud
Sourcefire

« Une stratégie de sécurité informatique complète et cohérente doit inclure le contrôle des utilisateurs à privilèges »

Ces dernières années, cyberdéfense et cybersécurité ont pris une place considérable dans la vie des entreprises et des particuliers. Les jours passent et les attaques s'amplifient. Elles sont toujours plus ciblées, diversifiées et étendues, et la cybercriminalité fait partie intégrante de notre vie quotidienne.

› Par Jean-Noël de Galzain

Historiquement, les éditeurs d'antivirus et de pare-feu ont pris le leadership du marché. Paradoxalement, ils ne traitent qu'une partie des problèmes ce qui se traduit par une augmentation du nombre d'incidents et de leur ampleur, malgré la croissance des budgets de sécurité informatique. En effet, un pan entier de la sécurité informatique reste méconnu : la gestion des utilisateurs à privilèges, qui répond au nom encore mal connu en France, d'Insider Threat ou gestion de la menace interne.

Une stratégie de sécurité complète et cohérente doit, certes, prévoir de se protéger contre les menaces provenant de l'extérieur mais également des risques qu'impliquent la liberté absolue dont jouissent les utilisateurs à privilèges.

UN UTILISATEUR À PRIVILÈGE, QU'EST-CE QUE C'EST ?

Un utilisateur à privilège, est, par définition, une personne dont les droits ont été élevés ou étendus sur le réseau informatique : droits d'accès, gestion des autorisations, administration des équipements et applications, modification, suppression ou transfert de fichiers, etc. L'utilisateur à privilèges peut être interne ou externe à une société. Ses droits lui sont délégués par le représentant légal de la société qui souvent n'est même pas au courant de ce risque. Par nature, l'utilisateur à privilèges a donc accès à des données sensibles et stratégiques pour l'entreprise aux secrets de l'entreprise et de ses salariés. Il a un droit de vie et de mort sur l'informatique de l'entreprise.

L'UTILISATEUR À PRIVILÈGES FAIT-IL TOUJOURS PARTIE D'UNE SOCIÉTÉ ?

Lorsqu'une société externalise la gestion d'une partie ou de l'ensemble de son informatique ou de ses équipements, les prestataires qui prennent la main à distance ou interviennent sur le réseau interne pour mener à bien des opérations de support ou de maintenance deviennent des utilisateurs à privilèges, et ce, bien qu'ils ne fassent pas partie

Pour aller plus loin sur ITPro.fr

Déléguer des tâches aux utilisateurs avec Forefront Identity Manager
bit.ly/deleguer-taches-utilisateurs

Le casse-tête des profils utilisateurs
bit.ly/casse-tete-profils

des effectifs de la société. Savez-vous par exemple quelles sont les autorisations d'accès d'un technicien qui vient réparer la photocopieuse IP ou la connexion réseau ?


Jean-Noël de Galzain

» Le marché français du Privileged User Management n'en est qu'à ses balbutiements malgré l'urgence.

En d'autres termes, externaliser revient, pour une entreprise et son dirigeant, à confier « les clés de la maison » à une personne inconnue, qui aurait accès à l'ensemble des pièces et du contenu des placards, avec la capacité de les fouiller, d'y prendre et remettre ce qu'il y trouve, en gérant lui-même les autorisations d'accès.

Si quelque chose est endommagé, disparaît ou est simplement dérobé après son passage, que faire ? Comment savoir ce qui a été fait ? Où y a-t-il eu un problème ? Quand ? De quelle manière ? Qui va payer les dégâts ? Comment vais-je pouvoir justifier l'incident ou le vol vis-à-vis des assurances ?

Pour le Clusif et son panorama 2012 des menaces informatiques, près de la moitié des entreprises de plus de 200 salariés en France, et des collectivités territoriales externalisent la gestion de leur Système d'information, 50% ne collectent pas les logs (pas de preuve), 20% ne changent jamais les mots de passe y compris lorsqu'un départ ou un changement de prestataire survient.

QUELS SONT LES RISQUES LIÉS AUX UTILISATEURS À PRIVILÈGES ?

De par leur statut, les utilisateurs à privilèges, au même titre que les utilisateurs « lambda » font peser des risques sur le réseau d'entreprises. On peut les classer en plusieurs catégories.

Les risques liés à l'erreur humaine

Comme n'importe quel utilisateur, l'utilisateur à privilèges reste un être humain, susceptible pour quelque raison que ce soit de commettre des erreurs sur un réseau ; seulement ces erreurs peuvent avoir des conséquences considérables sur la productivité, la réputation et le chiffre d'affaires de l'entreprise affectée.

Imaginons, par exemple, qu'après une erreur de manipulation lors d'une opération de télémaintenance, un prestataire externe provoque une panne sur le serveur d'un e-commerçant. Pour ce dernier, ce sont des pertes de chiffre d'affaires pendant toute la durée de la panne qu'il est nécessaire de réparer, mais avant cela d'en retrouver l'origine.

Ceci peut prendre un temps considérable, multiplier les dégâts mais également entacher sérieusement la réputation de l'e-commerçant définitivement. Entretemps, les clients iront se servir ailleurs. Désormais, avec les nouvelles réglementations, il sera nécessaire de communiquer sur un incident, avec un risque d'amende liée à la perte d'informations clients (données clients, numéros de carte bleue, ou encore, données de santé).

Dans un autre cas récent, des centaines de dossiers patients se sont retrouvés publiés sur Internet. C'est en tapant son nom par hasard dans un moteur de recherche qu'une personne a retrouvé l'intégralité de son dossier médical en libre consultation. Ce type de fuite de données peut provenir d'une erreur humaine (un prestataire externe commet une faute dans les process et laisse s'échapper ces données) ou d'un acte de malveillance qui illustre les risques liés aux utilisateurs à privilèges.

Les risques liés à la malveillance

L'utilisateur à privilèges reste un être humain. Ainsi, lorsqu'une collaboration professionnelle se finit en mauvais termes, il peut être tentant d'utiliser ses droits pour nuire à l'entreprise ou voler des informations stratégiques (fichiers clients, CB, secrets, …).

En 2012, c'est un sous-traitant de la société Toyota qui, après avoir été licencié, avait dérobé des informations relatives aux brevets industriels du constructeur japonais. Combien de bases clients dérobées, de messages divulgués ou d'informations recueillies grâce à des fichiers informatiques indûment téléchargés ?

Là encore, se pose la problématique de l'origine de la fuite. Qui a fait cela ? Quand et comment ? Pourquoi cette personne a-t-elle eu accès à ces données en particulier ? Peut-on empêcher un tel acte ou en garder la trace et comment ? Comment gérer cela en interne et avec les prestataires externes ?

Selon une étude Forrester, 50 % des utilisateurs à privilèges partent de leur entreprise ou sortent d'une mission d'infogérance avec des données sensibles. Comment peut-on donc évaluer ou mieux encore parler de gestion des risques sans traiter ce sujet ? Quand les hautes autorités de sécurité nationale mettront elles en garde contre ces risques béants ?

Heureusement, de plus en plus de DSI et de RSSI, pour répondre au contrôle interne ou à leurs directions générales, prévoient l'usage d'une solution qui réponde au problème de la gestion de la menace interne et des prestataires externes. Aussi ont-ils prévu l'intégration d'une solution de gestion des utilisateurs à privilèges dans leurs politiques de sécurité.

Le marché français du PUM (Privileged User Management) n'en est qu'à ses balbutiements malgré l'urgence. Il est urgent de préconiser la protection contre les menaces provenant de l'extérieur du réseau. Elles sont connues et désormais très bien circonscrites grâce à des solutions comme l'anti-virus, le firewall, l'IPS, l'IDS etc. Il est également indispensable de compléter ces dispositifs par des solutions internes de contrôle des utilisateurs à privilèges.

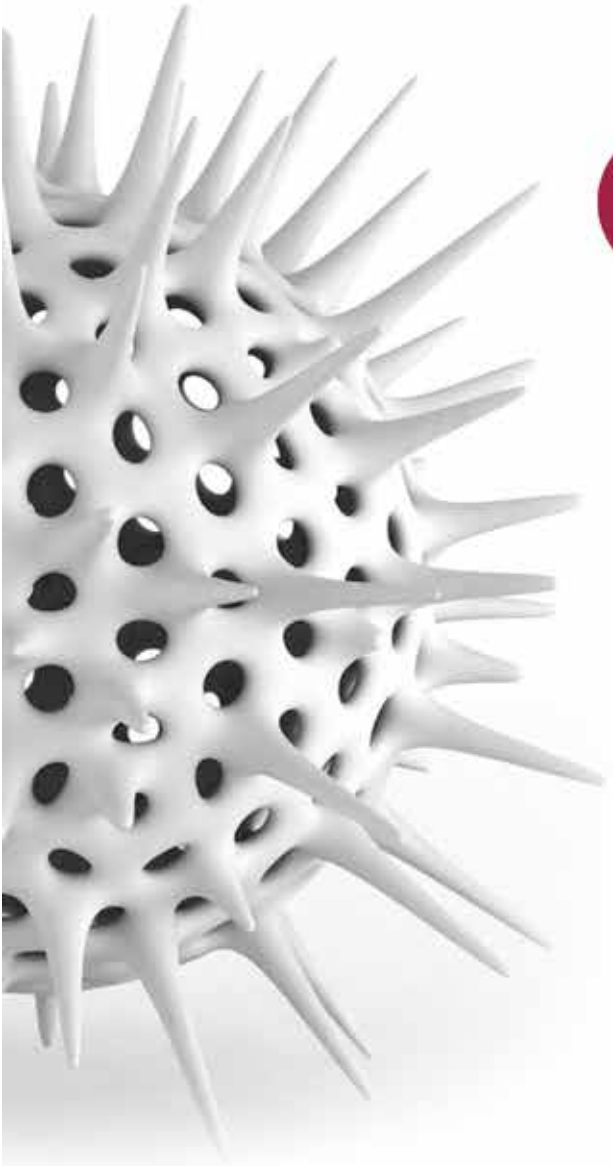
Cependant, ces solutions souffrent d'une mauvaise réputation : trop souvent, celles-ci sont perçues comme des produits visant purement et simplement à surveiller les utilisateurs à privilèges. Contre toute attente, elles permettent surtout de dédouaner les utilisateurs en apportant une preuve tangible et concrète de l'origine de l'incident. ■

Jean-Noël de Galzain
Fondateur de WALLIX
www.wallix.com

CHECK POINT
RAPPORT SÉCURITÉ 2013

900 SYSTÈMES D'INFORMATION D'ENTREPRISES ET 120 000 HEURES DE TRAFIC ANALYSÉS !

Ce que révèle notre étude à propos des réseaux d'entreprise :



75 % ACCÈDENT À DES SITES MALVEILLANTS

63 % SONT INFECTÉS PAS DES BOTS

54 % SUBISSENT DES FUITES DE DONNÉES

47 % UTILISENT DES ANONYMISEURS

TÉLÉCHARGEZ LE RAPPORT COMPLET

en pdf (QR code) ou demandez un exemplaire relié à Danièle Jouin

Téléphone : 01 55 49 12 00

Email : danielej@checkpoint.com

Check Point est distribué par COMPUTERLINKS

Check Point
SOFTWARE TECHNOLOGIES LTD.

Faut-il repenser sa stratégie sécurité en termes de fuite d'informations ?

› Par Benoit Micaud

Dans le monde de la sécurité de l'information, le modèle de la défense en profondeur a été, ces dernières années, le modèle privilégié par une grande majorité des entreprises. Ses principes de base sont de positionner, entre l'agresseur et les informations importantes de l'entreprise, un ensemble de mesures de sécurité successives devant permettre d'arrêter, de ralentir, éventuellement d'égarer l'agresseur et, dans le même temps, de détecter puis de réagir à l'agression avant que celle-ci n'atteigne les informations sensibles.

Ce modèle, s'il n'est pas encore complétement désuet, doit, a minima, être complété dans un monde où la donnée critique peut se retrouver dans une tablette ou un smartphone personnel d'un dirigeant, accessible via Internet pour des commerciaux itinérants, ou qui peut être exploitée par un infogérant…

La dernière évolution en date et pas la moins dangereuse, est que la donnée critique peut-être partagée, échangée, et traitée dans le « Nuage » par une direction métier, attirée par une optimisation de ses coûts opérationnels. Au vu de ces évolutions, quelle est l'efficacité de notre défense avec ses firewalls, ses IDS, ses proxy, ses antivirus… ? Face à ces nouveaux usages multiformes, multicanaux, multi-infrastructures, peut-on encore parler de défense en profondeur alors que la plupart des équipements de protection ne sont plus traversés ?

Dans le monde distribué et mutualisé qui se dessine, il va être nécessaire de revoir une grande partie de nos fondamentaux en termes de fuite d'informations car celle-ci sera elle-même multiforme et distribuée. La sécurité devra forcément, à terme, être portée également par l'information et plus seulement par les droits des utilisateurs accédant. Des mécanismes de sécurité comme le chiffrement et le scellement viendront compléter cet arsenal. Une fois positionnés, les attributs sécurité d'une information devront la suivre quels que soient la manière dont elle est utilisée, l'endroit où elle est stockée, les moyens permettant de la véhiculer... Les attributs de sécurité de l'objet informationnel, de l'objet technique, de l'objet utilisateur… devront être comparés et le droit d'usage autorisé en fonction de cette comparaison. Les tentatives de mise en place de solution de DLP, première étape dans cette évolution, ont montré les difficultés auxquelles peuvent être confrontées les métiers dans la définition des comportements vis-à-vis de leurs biens informationnels. Il est plus simple de donner un droit d'usage à un individu ou à un groupe d'individu que de fixer quelles conditions d'utilisation d'une donnée sont licites et par extension celles qui sont anormales. La plupart des solutions sont utilisées pour répondre à des besoins de traçabilité et n'ont pas encore évolué vers le blocage, probablement par peur des problématiques pouvant en découler (traitement non effectué, envoi important bloqué, VIP n'accédant plus en cas de crise…).


Benoit Micaud

› La sécurité devra forcément, à terme, être portée également par l'information et plus seulement par les droits des utilisateurs accédant.

En synthèse, notre modèle de prise en compte de la fuite d'information doit évoluer vers une protection positionnée sur l'information. Elle nécessite une identification des usages licites des informations critiques de l'entreprise. Cette étape passe nécessairement par une prise en compte voir une formalisation des processus métier d'utilisation de ces informations critiques. ■

Benoit Micaud,
Consultant Sécurité Sénior
Lexsi

Pour aller plus loin sur ITPro.fr

Comment prévenir la fuite des données
www.itpro.fr/a/comment-prevenir-fuite-donnees

Leaks ! Protéger rapidement vos données sensibles d'entreprise
bit.ly/proteger-donnees-sensibles

PAESSLER

COMSOFT direct
Bechtle's Software Specialist

Comment choisir la solution de surveillance réseau adéquate ?

Pour que son infrastructure informatique lui donne entière satisfaction, toute entreprise doit pouvoir compter sur un réseau haute performance.

Pour maintenir la fluidité des procédures, tous les processus doivent **fonctionner de manière fluide**, y compris les communications internes et externes entre sites de l'entreprise, ainsi qu'avec les clients et partenaires. Les dysfonctionnements et pannes des processus opérationnels provoquent **facilement des pertes de temps et surtout d'argent**. Voilà pourquoi il est vivement recommandé de s'équiper **d'un logiciel de surveillance réseau** qui veille constamment au bon fonctionnement des processus sur le réseau, effectue des analyses et **alerte l'équipe informatique** dès qu'une erreur se produit ou que les seuils critiques sont dépassés.

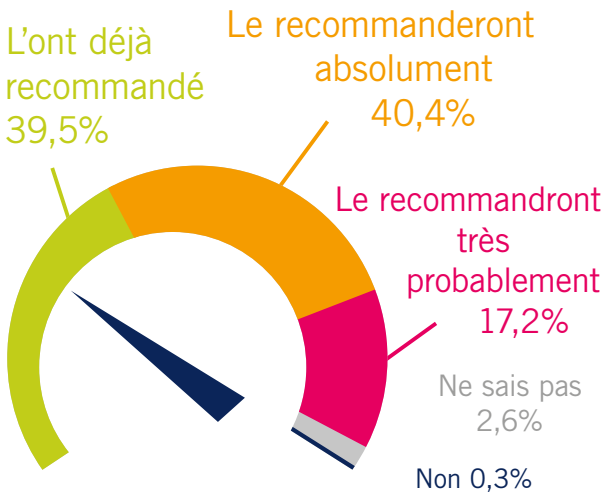
Une telle **solution de surveillance réseau** permet à l'administrateur d'intervenir rapidement, y compris à distance, s'il n'est pas sur place. Et comme le marché propose de nombreux outils et solutions différents, il convient de sélectionner avec soin la solution la mieux adaptée.

N'hésitez pas à télécharger gratuitement ce livre blanc qui fait le point sur les nombreuses options qu'une solution de surveillance réseau peut proposer et explique quels critères doivent guider la décision.

comsoft.orig-in.com/paessler-surveillance.html

PRTG Network Monitor ...

- est une surveillance simple, fiable et globale de votre réseau, déjà testée et expérimentée dans plus de 150 000 installations à travers le monde.
- est une solution logicielle unique supervisant l'ensemble de votre réseau, y compris les périphériques, les applications, le trafic et la disponibilité.
- est évolutive, de haute disponibilité, facile à utiliser et s'adaptant à votre budget grâce à un modèle de licence clair et equitable.
- est capable de surveiller plusieurs sites à partir d'une installation central.
- PRTG surveille votre réseau 24/7 pour vous avertir des problèmes avant qu'ils ne surviennent !



Testez dès maintenant la version d'essai gratuite de PRTG Network Monitor pendant 30 jours et avec toutes les fonctionnalités.

https://shop.paessler.com/trial/prtg/3a8a

PRTG NETWORK MONITOR

COMSOFT direct
Bechtle's Software Specialist
Comsoft France
Tél. 0825 07 06 07
infos@comsoft.fr

AD/20130527/FR

La sécurité d'Android en question

Le système d'exploitation de Google est aujourd'hui le numéro un des smartphones. Une popularité qui va de pair avec un intérêt grandissant des hackers.

› Par Guillaume Rameaux

Plus de 30 millions de smartphones Android infectés en 2012. Dans son dernier rapport annuel de sécurité, l'éditeur NQ Mobile tire la sonnette d'alarme sur la recrudescence de malwares ciblant le système d'exploitation mobile de Google. La plateforme qui connait une croissance fulgurante attire de plus en plus les pirates informatiques. Selon des chiffres publiés par ABI Research, il y aura à la fin de l'année près de 800 millions de terminaux Android actifs dans le monde contre environ 300 millions début 2012.

Une situation que l'on surveille également de très près dans les laboratoires McAfee. Le fournisseur de solutions de sécurité voit apparaître 80 nouveaux malwares par jour sur cette plateforme. « C'est une problématique réelle pour les entreprises qui ont tendance à privilégier le monde Android essentiellement en raison du prix d'acquisition du matériel, indique Laurent Maréchal, responsable des offres mobilité pour l'Europe du Sud. Notre politique est de pouvoir accompagner un business dans un périmètre sécuritaire maîtrisé au sein d'un environnement hétérogène ». Et la tâche n'est pas aisée en ce qui concerne Android puisqu'il existe entre 40 et 50 versions différentes de l'OS si l'on prend en compte les différentes releases, les versions smartphones et tablettes ainsi que les surcouches appliquées par les constructeurs

Pour aller plus loin sur ITPro.fr

ROOMn – Kaspersky :
« Une explosion de malwares sur Android »
bit.ly/explosion-malwares-android

La menace s'accentue sur Android selon AVG
bit.ly/menace-android-avg


Laurent Maréchal

» On assiste en ce moment à un phénomène de consumérisation des attaques.

comme Touchwiz chez Samsung ou Sense chez HTC.

Pour combler les failles du système, l'éditeur mise donc avant tout sur la surveillance des applications. Ces dernières véhiculeraient 90 % des malwares et il serait particulièrement aisé, aujourd'hui, de développer une application malveillante. « On assiste en ce moment à un phénomène de consumérisation des attaques. On peut très facilement trouver sur internet des outils pour déployer en cinq minutes une application capable de se connecter à un numéro surtaxé à l'étranger sans que l'utilisateur en prenne connaissance ». Moins de cinq lignes de code suffisent à développer un malware pour initier ces communications et générer de l'argent simplement puisque le titulaire de la ligne, qu'il s'agisse d'un particulier ou d'une entreprise, peut rapidement se retrouver avec des factures de plusieurs milliers d'euros.

UN MOBILE EFFACÉ AVEC UN SIMPLE SMS

Autre problématique à prendre en compte, les attaques de type 0-day qui gagnent les environnements mobiles. « Ces menaces sont très difficiles à détecter pour un antivirus classique basé sur des signatures », souligne le responsable McAfee. C'est pourquoi la filiale d'Intel a intégré à ses produits la GTI (Global Threat Intelligence), une base de données qui permet de faire de la réputation applicative via des informations récoltées auprès des clients McAfee du monde entier. L'idée est d'analyser le comportement d'une application, de vérifier à quelles données elle accède, si elle en envoie à des serveurs tiers, dans quel pays, s'il s'agit d'une application nouvelle Tout cela afin de lui donner une note pour évaluer son niveau de risque. Cette note sert ensuite à alerter l'utilisateur ou l'administrateur du terminal en cas de risque élevé.

« Il faut revoir les facultés d'un antivirus porté vers le monde Android, poursuit Laurent Maréchal. Les solutions traditionnelles ne sont pas suffisantes ». Avec son offre VirusScan Mobile, McAfee capitalise donc sur son expérience du monde PC et la transpose dans l'univers Android tout en prenant en compte certaines spécificités comme la batterie limitée des terminaux par exemple. McAfee affirme avoir relevé le défi avec une solution ne consommant que 3 % de l'autonomie globale de l'appareil. Ensuite, certaines sources de problèmes propres aux smartphones doivent impérativement être prises en compte. C'est le cas notamment des SMS.

En fin d'année dernière, certains smartphones Samsung sous Android avaient été pointés du doigt en raison d'une faille exploitant les codes USSD. Ces codes sont des suites de caractères qui permettent d'activer un service comme le #123# chez Orange, qui sert à suivre sa consommation, ou le *#06#, qui permet de connaître son numéro IMEI. Si ces derniers sont inoffensifs pour les appareils, d'autres codes utilisés par les opérateurs peuvent permettre par exemple de bloquer à distance la carte SIM d'un appareil volé ou encore d'effacer toutes les données du téléphone. C'est ce dernier code qui a été révélé sur la toile et démonstration a été faite lors de la dernière conférence ekoparty qu'il était possible de réaliser un wipe d'un terminal simplement en envoyant ce code par SMS. « Avec ce type de faille, tout un chacun est susceptible de perdre les données professionnelles et personnelles stockées sur son téléphone ». C'est pour cette raison que VirusScan analyse également le contenu des SMS reçus afin de détecter toute menace qu'ils pourraient contenir.

LE DANGER NFC

De nouveaux besoins sont également créés par les constructeurs comme le NFC, largement poussé par Google pour se différencier de son concurrent Apple. Cette technologie permet de faire du paiement sans contact. Des entreprises de la grande distribution testent actuellement le paiement via smartphone, de même que la RATP étudie la possibilité d'utiliser son téléphone pour payer ses déplacements. « Tout cela amène à penser que, bientôt, nous verrons des cyber-pickpockets dans le métro, indique Laurent Maréchal. Le NFC est déjà cassable avec des technologies utilisées par des entités gouvernementales. La DCRI dispose d'outils permettant d'interroger le contenu d'un périphérique NFC à une distance de 7 mètres. Ce n'est évidemment pas sur le marché mais à la vitesse où l'information circule, il est risqué à mon sens d'utiliser son téléphone pour payer une transaction ». Selon les derniers chiffres publiés par l'Observatoire du NFC et du sans contact, la France compte actuellement plus de 3 millions de terminaux compatibles NFC contre 1 million en juin 2012. Si leur utilisation est encore minime aujourd'hui, IDC prévoit que le montant des paiements réalisés par mobile (NFC et m-commerce confondus) devrait atteindre 1 000 milliards de dollars d'ici 4 ans. ■

Les cyber-menaces ne sont pas suffisamment prises au sérieux par les entreprises

› Par Denis Gadonnet

Aujourd'hui, les cyber-attaques de nouvelle génération sont omniprésentes et s'avèrent particulièrement dangereuses pour les entreprises. En effet, ces menaces APT (Advanced Persistent Threat) sont caractérisées par la combinaison de différentes techniques d'attaques qui, associées entre elles, permettent de générer des attaques sophistiquées (« avancées »), avec des intrusions durables et quasiment indétectables par les outils de sécurité informatique traditionnels.

Et le risque continue d'augmenter : d'après notre dernière étude[1] sur les menaces APT, basée sur des données recueillies à partir de 89 millions d'évènements survenus au second semestre 2012, les entreprises sont victimes d'un malware toutes les trois minutes en moyenne.

Les principales techniques utilisées par les cybercriminels sont :
- Le phishing (technique « d'hameçonnage » visant à usurper l'identité d'une personne en récupérant des informations confidentielles par le biais de sites web ou des liens frauduleux).
- La pièce-jointe corrompue.
- Le click-jacking (détournement de clic pour pousser un internaute à fournir des informations confidentielles ou à donner accès à son ordinateur à distance).
- Les logiciels piégés.
- Le partage de réseau piégé (serveur FTP, intranet).
- Les supports amovibles (type clé USB, disques durs externes, etc.).

[1] « Advanced Threat Report », publié le 4 avril 2013.

Pour aller plus loin sur ITPro.fr

McAfee s'inquiète d'une course au cyber-armement
bit.ly/course-cyber-armement

85 % des infrastructures critiques victimes d'une infiltration réseau
bit.ly/infrastructures-infiltration-reseau


Denis Gadonnet

» La lutte contre les cyber-menaces doit être prise au sérieux par les entreprises.

La technique de hameçonnage est la méthode la plus utilisée en matière d'intrusion. Certains formats de fichiers sont également privilégiés : 92 % des fichiers frauduleux sont acheminés sous format .Zip. Nous avons aussi observé que les attaques sont désormais initiées par les fichiers. DLL en remplacement du format de fichier d'application .EXE.

Ces techniques traditionnelles sont connues, cependant, c'est la manière dont elles sont employées par les pirates qui a évolué, tout comme leurs compétences techniques, ou encore leurs objectifs. Le but des cyber-attaques actuelles est de générer un impact majeur sur l'activité d'une organisation : pas forcément en exploitant les failles existantes, mais en les contournant de manière à ne pas éveiller les soupçons, et permettre ainsi de passer les barrières de sécurité traditionnelles.

L'enjeu est de s'introduire dans le système sans se faire repérer, afin de disposer du temps et de l'amplitude nécessaire pour leurs attaques, selon leurs objectifs : vol d'information, perturbation ou même destruction du système.

Car les motivations des cybercriminels ont aussi changés : il ne s'agit plus seulement de « perturber » l'activité d'une organisation, mais de lui porter préjudice, que ce soit en termes d'image, de réputation, de propriété industrielle/intellectuelle ou en matière financière. Les pirates sont aujourd'hui des « professionnels » qui mettent en œuvre des campagnes de cyber-attaque abouties, en utilisant des techniques évoluées.

Le contexte géopolitique sensible et la forte concurrence entre les entreprises viennent renforcer les initiatives malveillantes à l'égard des gouvernements, des institutions internationales ou de grandes multinationales. Les cyber-attaques se démocratisent, allant du cyber-espionnage, à la cyber-escroquerie en passant par le simple déni de service (DDoS), et avec un nombre toujours plus important d'outils développés par les pirates eux-mêmes et mis à disposition de leurs homologues au niveau international, la prévention devient de plus en plus compliquée.

Toutefois, en plus de connaitre les nouvelles méthodes utilisées par les cybercriminels, nous savons maintenant cartographier les mouvements des cyber-attaques : d'où elles proviennent, qui elles ciblent et par où elles transitent, grâce notamment au suivi des serveurs CnC (« Command and Control »).

La dernière étude[2] de FireEye dans ce domaine indique que les cyber-menaces sont aujourd'hui globalisées : 184 pays, soit 93 % des pays du monde, hébergent des hubs de communication ou des serveurs de type CnC permettant d'initier des campagnes malveillantes, qu'elles soient dirigées vers l'extérieur ou dans le pays même où les serveurs sont installés.

Si aucun pays n'est épargné, la majorité des cyber-attaques semble cibler les pays où les entreprises technologiques sont les plus présentes, comme aux Etats-Unis, en Corée du Sud et au Japon.

L'Asie et l'Europe de l'Est ont également été identifiées comme un fort point de concentration d'initiation de cyber-attaques. Toutefois, la surveillance des canaux de communication malveillants indique que les points de départ des attaques ne proviennent pas toujours de l'extérieur mais plutôt de réseaux internes ; comme les techniques d'évasion de données en communication intra-pays se remarquent moins, les hackers parviennent aujourd'hui à mettre la main sur des serveurs locaux, masquant ainsi les prémices d'une cyber-attaque.

Les conséquences des cyber-attaques peuvent donc s'avérer dramatiques, que ce soit pour les institutions gouvernementales ou les opérateurs d'importance vitale (OIV), ou pour les entreprises aux activités moins critiques.

La lutte contre les cyber-menaces doit être prise au sérieux par les entreprises, qui ont tendance à en minimiser les répercussions, qu'elles soient financières, liées à la propriété intellectuelle de l'entreprise ou bien à sa réputation. ■

Denis Gadonnet
Directeur Commercial Europe du Sud
FireEye

[2] « Advanced Cyber-attack Landscape », publié le 23 avril 2013.

La gouvernance des flux de données : la sécurité au cœur des échanges numériques

› Par Jean-Claude Bellando

Pour l'entreprise numérique, la création de valeur passe par l'échange de données au travers des différents écosystèmes auxquels elle est connectée. Sous la pression de la numérisation et des nouveaux usages, la frontière de l'entreprise s'est éloignée de ses quatre murs. À ce stade, la sécurité électronique de l›entreprise ne peut plus se contenter de solutions visant à bloquer l'accès à son périmètre ; refuser l'accès c'est déjà refusé de collaborer.

De fait, les échanges sont omniprésents, ils sont multiformes et interviennent tout au long du déroulement des différents processus de l'entreprise. Chaque type d'échange pose ses propres contraintes et exigences en termes de sécurité.

La sécurité doit s'appliquer à tous les échanges, tout en s'adaptant à chacun des différents modes d'échange utilisés. Pour être efficace, sans être ni trop légère, ni trop pesante, la réponse sécuritaire ne peut pas être unique, elle doit être adaptée à la nature de l'échange.

Au-delà des modèles d'infrastructure à base de passerelles, de DMZ,

Pour aller plus loin sur ITPro.fr

Sécuriser les échanges de fichiers dans le cloud en trois étapes
bit.ly/securiser-fichiers-cloud

Protection systématique des échanges électroniques
bit.ly/protection-echanges-electroniques

de «reverse proxy» et autres dispositifs disponibles sous forme d'appliances, la gouvernance des flux de données permet de répondre de façon argumentée et systématique à la problématique de sécurité des échanges.

Ainsi, un échange entre applications au sein de l'entreprise peut paraître anodin, mais pose déjà les contraintes suivantes :

• Les deux applications doivent avoir les droits nécessaires et les accès aux données échangées.
• Les données échangées contiennent des informations de types données privées (par exemple des coordonnées bancaires de clients). Celles-ci doivent être chiffrées de bout en bout.
• Enfin, l'échange doit être supervisé, de sorte à pouvoir lever une alerte en cas de corruption des données, des pistes d'audit doivent permettre de retracer a posteriori l'échange et expliquer l'ensemble des actions intervenues durant celui-ci.

La vocation de la gouvernance des flux de données est justement de pouvoir répondre à trois questions.


Jean-Claude Bellando

> La gouvernance des flux de données permet donc une gestion dynamique des enjeux de sécurité liés aux échanges de données.

1. Qui interagit avec qui ?

Chacun des participants de l'échange peut être au choix : une personne (employé, client, partenaire) ou une application dans un data center de l'entreprise, sur un appareil mobile, sur le Cloud, chez un partenaire. Chacun présentant des contraintes de sécurité, des droits et un mode d'authentification différents.

Ici, les services pertinents comprennent les fonctions d'identité et de gestion des accès (IAM), de gestion des cycles de vie des certificats, OAuth, LDAP, …

2. De quelle interaction s'agit-il ?

Une fois les participants identifiés, il s'agit de définir le type d'interaction à gérer et donner le motif de l'interaction : échange de facture, de bons de commande… Cette définition peut se limiter au strict échange de données mais peut également contenir les traitements associés à l'échange. S'agissant de sécurité, des phases d'archivage, de journalisation, chiffrement et de décision humaine peuvent être ajoutée.

En fonction des ces informations, des directives et des règles associées à cet échange vont pouvoir être créées et pourront être appliquées systématiquement.

Les services associés à cette phase contiennent les fonctions de chiffrement, signature, studios de configuration et définition de règles et directives…

3. L'interaction se déroule-t-elle comme nécessaire ?

Une interaction réussie est celle qui se déroule comme prévue en accord avec l'ensemble des définitions et des contraintes auxquelles elle est soumise. C'est ici que seront définis les alertes et rapports permettant de suivre l'application des directives ainsi que les flux de données par eux-mêmes.

Les services utilisés à ce stade s'appuient sur des outils de type tableaux de bords et supervision, mais aussi de gestion de journaux d'audit sécurisés, …

Dès lors qu'on sait répondre à ces trois questions les enjeux de sécurité apparaissent immédiatement et peuvent être gérés de façon systématique.

Aujourd'hui, l'entreprise est amenée à appuyer son activité sur des écosystèmes étendus. D'une part, elle doit se doter de moyens d'échanger rapidement des données avec chacun des participants des différents écosystèmes dont elle dépend et qui passent désormais, par la publication de services via des API. D'autre part, elle ne peut pas considérer l'ensemble des participants aux échanges de données de façon uniforme.

Elle doit proposer des niveaux de services d'accès à ses données en fonction des contrats qu'elle a avec chacun.

La gouvernance des flux de données permet donc une gestion dynamique des enjeux de sécurité liés aux échanges de données. ■

Jean-Claude Bellando
Director
Product Solution Marketing
Axway

Le signalement tardif des terminaux perdus

La disparition d'un équipement informatique peut être grave pour une entreprise. Surtout si celui-ci n'est signalé qu'après plusieurs jours.

> Par Guillaume Rameaux

Tablette volée ou smartphone oublié à la terrasse d'un café, la perte d'un terminal devient de plus en plus problématique à mesure que les informations stockées à l'intérieur deviennent plus nombreuses et critiques. Alors que les usages mobiles explosent, les sociétés tentent d'assurer à leurs employés un accès distant à leurs informations et applications professionnelles. L'appareil mobile est donc aujourd'hui une véritable porte d'entrée vers le système d'information (SI) et les entreprises tout comme les salariés européens ne semblent pas en avoir pleinement conscience. C'est en tout cas ce qui ressort de l'étude menée par TNS Infratest pour Kaspersky.

D'après les chiffres publiés par l'éditeur de solutions de sécurité, seuls 21 % des responsables informatiques pensent être informés dans l'heure qui suit la perte d'un équipement de l'entreprise et ils sont 12 % à estimer que ce délai est supérieur à une journée. Globalement, les entreprises ne sont que 6 % à considérer comme très grave la perte d'un smartphone ou d'une tablette. Parmi les mauvais élèves de l'étude, les salariés belges sont 19 % à indiquer attendre au moins trois ou quatre jours avant de signaler la disparition et le constat est similaire aux Pays-Bas (17%) ou en Allemagne (16%). Une personne malintentionnée aurait alors tout le temps d'extraire les contacts, mails ou tout autre document stocké en interne, voire d'utiliser les applications installées pour atteindre des données directement sur le SI ou dans le cloud.

Pour aller plus loin sur ITPro.fr

Top 5 des récupérations d'ordinateurs portables volés
bit.ly/top-recuperation-ordinateurs

Les faiblesses des terminaux mobiles
www.itpro.fr/a/faiblesses-terminaux-mobiles


Tanguy de Coatpont

» Seuls 21 % des responsables informatiques pensent être informés dans l'heure qui suit la perte d'un équipement de l'entreprise.

« Les entreprises et les employés ont peu conscience que perdre ou se faire voler un smartphone ou tablette peut avoir des conséquences graves pour l'entreprise, indique Tanguy de Coatpont, Directeur Général de Kaspersky en France. La conséquence directe, c'est la perte de données et le risque de voir le SI compromis à cause d'un terminal non sécurisé. Le problème étant que lorsqu'on n'est pas conscient d'un problème, on ne met pas en œuvre les solutions pour lutter contre ».

LA FAIBLESSE DU CODE PIN À QUATRE CHIFFRES

Et les 1700 responsables informatiques interrogés ne sont effectivement que 39 % à admettre qu'une technologie comme le chiffrement des données constitue une méthode plus efficace qu'un simple mot de passe. « Un cybercriminel chevronné n'a besoin que de quelques minutes pour contourner une protection par mot de passe à 4 chiffres telle que celle utilisée sur la plupart des appareils, notamment les smartphones », souligne David Emm, chercheur senior en sécurité chez Kaspersky. C'est pourquoi il est fortement recommandé aujourd'hui d'employer un code PIN d'au moins six chiffres afin d'apporter une première barrière de sécurité. Pour les entreprises, des solutions de gestion des terminaux existent afin d'obliger l'utilisateur du terminal à rentrer un mot de passe fort. D'autres fonctionnalités permettent de localiser l'appareil, le bloquer ou l'effacer à distance.

Ces outils peuvent toutefois être difficiles à mettre en œuvre dans le cas d'un terminal personnel utilisé par l'employé pour travailler. L'une des réponses apportées à ce phénomène BYOD (Bring Your Own Device) est le principe de conteneurisation. Il s'agit alors de gérer de façon indépendante sur le terminal les applications professionnelles et personnelles et ainsi de permettre, en cas de problème, la suppression des données sensibles de l'entreprise sans toucher à la partie privée du téléphone ou de la tablette. ■

Éviter les conflits informatiques grâce à une base de référence de gestion efficace

> Par Rich Makris

Amazon et Google ont fait la une en 2012 pour leurs spectaculaires interruptions de service, qui ont démontré combien les entreprises sont vulnérables aux pannes informatiques, qui peuvent avoir des répercussions négatives sur les ventes et la productivité.

C'est pourquoi, avant de s'attaquer à des grands projets, les responsables informatiques et des réseaux feraient bien de définir une base de référence pour comprendre exactement où ils en sont. Les réseaux devenant de plus en plus complexes (virtuels ou physiques, filaires ou sans fil, etc.), une pression s'exerce pour améliorer les performances et la disponibilité des applications stratégiques pour l'entreprise et celles destinées à la clientèle.

Les professionnels de l'informatique gagneraient considérablement à définir quatre axes principaux pour un meilleur contrôle de leur réseau :

- Une base de référence d'inventaire : vous ne pouvez pas contrôler les choses dont vous n'avez pas connaissance.
- Une base de référence des performances : commencez par les cinq principaux points : UC, mémoire, disque, utilisation de l'interface et temps de latence ping, puis mesurez la consommation des principales applications et les seuils optimums.
- Une base de référence de configuration : voyez comment les configurations en vigueur influent sur la sécurité, la conformité et le contrôle global du réseau.
- Une base de référence relative à la bande passante et au flux de données : effectuez des mesures sur le réseau pour savoir quand et comment la bande passante est consommée.

La capacité d'une entreprise à se développer repose sur la disponibilité et les performances informatiques, mais de nombreuses organisations refusent pourtant de reconnaître leur impact sur les résultats, jusqu'à ce qu'il soit trop tard. Pensez à des situations telles que :

- L'application de commerce électronique est lente, ou pire, n'est plus disponible du tout.
- La messagerie de l'entreprise n'est plus connectée, ce qui nuit gravement à la productivité.
- Des applications stratégiques pour l'entreprise, comme SalesForce.com ou SAP ne répondent plus.

Les pertes financières pourraient être accablantes. Qu'elles soient mineures ou majeures, les interruptions informatiques nous touchent tous. Au fur et à mesure que les environnements informatiques deviennent de plus en plus complexes, les services informatiques sont de plus en plus occupés à optimiser la disponibilité et les performances. Or, l'optimisation de l'infrastructure passe par la définition d'une base de référence informatique. Elle sert de référence pour comprendre : (a) comment le réseau, les applications et l'infrastructure se comportent en termes de performances (b) où et pourquoi les problèmes de performances surgissent, et (c) quelles sont les étapes à mettre en œuvre pour l'optimisation. La création d'une base de référence doit inclure quatre principaux éléments : inventaire, performances, configuration et flux.

BASE DE RÉFÉRENCE D'INVENTAIRE

Alors que la majorité des responsables informatiques connaissent bien l'infrastructure de base, les équipements en périphérie leur sont moins familiers.

Les équipements inconnus compliquent la gestion du réseau, car ils peuvent consommer beaucoup de ressources et nuire

Pour aller plus loin sur ITPro.fr

Dossier Haute-Disponibilité
www.itpro.fr/t/haute-disponibilite/

Comment sécuriser votre infrastructure réseau ?
bit.ly/comment-securiser-reseau


Rich Makris

> La sécurité, la conformité et le contrôle sont en tête de la liste des priorités des directeurs informatiques.

aux performances informatiques cruciales. Trois principaux axes doivent être pris en compte pour mieux contrôler le réseau : le matériel, les systèmes et les applications. Tous les composants sont-ils à jour, avec les dernières versions installées ? Tous les correctifs de sécurité ont-ils été appliqués ? Comment les composants de l'infrastructure sont-ils reliés aux autres ? Il est particulièrement important de comprendre les interdépendances au sein du réseau pour pouvoir détecter les problèmes et les résoudre rapidement. Si un utilisateur reconfigure un routeur en le déplaçant d'un sous-réseau à un autre, et crée une boucle dans le réseau, ce changement peut être catastrophique pour l'ensemble du réseau. Constituer une base de référence d'inventaire facilite la détection et la résolution des problèmes, et aide à contrôler les coûts en repérant les ressources sous-utilisées, qui peuvent être redéployées.

DÉFINIR DES SEUILS DE PERFORMANCE

Cinq éléments principaux doivent être pris en compte pour créer une base de référence de performance : l'UC, la mémoire, le disque, l'interface d'utilisation et le temps de latence ping.

Les administrateurs de réseau doivent savoir combien leurs applications et leurs services cruciaux consomment de ces cinq éléments. Plus important, ils doivent connaître les seuils optimums. Les seuils de performance jouent un rôle crucial. Si un élément de réseau consomme 98 % des ressources de l'UC, il y a fort à parier qu'il est sur le point de tomber en panne, ce qui aura une incidence sur la disponibilité du réseau et les performances. L'essentiel pour établir une base de référence de performance est de comprendre quels sont les seuils acceptables pour chaque élément et serveur du réseau, et de mettre en place un système en temps réel d'alerte chaque fois qu'un seuil n'est pas respecté.

BASE DE RÉFÉRENCE DE CONFIGURATION

La sécurité, la conformité et le contrôle sont en tête de la liste des priorités des directeurs informatiques. Ils constituent également les éléments essentiels d'une base de référence. Est-ce que les éléments du réseau répondent aux critères suivants ?

- Est-ce qu'ils utilisent tous des configurations autorisées ?
- Toutes les fonctions de sécurité sont-elles activées ?
- Les mots de passe par défaut sont-ils toujours utilisés ?
- Pouvez-vous générer un journal d'audit de tous les changements de configuration ?

Les manquements dans ce domaine pourraient se traduire par des failles de sécurité et des non-conformités.

Les services informatiques à la pointe font appliquer des politiques de contrôle des changements de configuration strictes. Ils archivent les configurations autorisées, reçoivent des alertes en cas de modification des configurations et génèrent des rapports répondant à ces questions cruciales : qui, quoi et quand. Dans ces conditions, les actions correctives et le respect de la conformité sont beaucoup plus faciles.

BASE DE RÉFÉRENCE RELATIVE À LA BANDE PASSANTE ET AU FLUX DE DONNÉES

Cette base de référence aide les professionnels de l'informatique à comprendre la consommation des ressources du réseau et de la bande passante. Une base de référence complète du flux détaille l'utilisation des ressources et de la bande passante par les utilisateurs, les services et les applications.

L'optimisation de la bande passante et des ressources du réseau est essentielle pour améliorer les performances et la productivité. Les responsables informatiques doivent comprendre ce qui se passe sur le réseau et savoir quel pourcentage de bande passante est consommé. L'objectif final est de s'assurer que les applications stratégiques de l'entreprise disposent de la largeur de bande dont elles ont besoin pour fonctionner au maximum de leurs performances.

Savoir quel pourcentage de ressources du réseau les employés utilisent a également une incidence sur le budget. De loin, l'entreprise peut sembler avoir besoin de largeur de bande plus importante, alors qu'en réalité elle pourrait en économiser 30 % en détectant les utilisations illicites de gros consommateurs de bande passante, comme YouTube. De nos jours, les environnements informatiques sont dynamiques et complexes. Des changements se produisent tous les jours qui affectent les performances et la disponibilité. Toutefois, une base de référence des ressources et des seuils de performance est utile aux services informatiques pour améliorer en temps réel les performances et l'efficacité du réseau. ■

Rich Makris
Ingénieur commercial senior
Ipswitch, Inc.

Internet, évolution des menaces et des systèmes de défense

› Par Emmanuel Macé

Il y a encore quelques années, les mots « sécurité » et « cloud » ne pouvaient apparaître dans la même phrase.

Avec l'exposition croissante des entreprises sur Internet et l'émergence de nouvelles menaces sur le Web, adopter une stratégie de défense distribuée apparaît aujourd'hui comme une évolution naturelle.

Dans son rapport « Predicts 2013: Security Solutions »[1], Gartner prévoit qu'en 2015, 10% des solutions de sécurité des entreprises seront délivrés via Internet ce qui soulève de fait de nombreuses interrogations : Pourquoi aujourd'hui les méthodes de protection traditionnelles ne suffisent plus ? Pourquoi de nouveaux moyens de protection émergent-ils? Quelles sont les raisons qui poussent de plus en plus d'entreprises à adopter un système de défense dans le cloud ?

NOUVEAUX PROFILS DES MENACES

Cet essor est, en parti, lié à l'apparition de nouvelles menaces qui planent sur les sites et applications publiés sur Internet. En 2012, le nombre d'attaques par déni de service distribuées (DDoS) constatées sur la plateforme Akamai a augmenté de plus de 200 % par rapport à l'année précédente[2]. Cette explosion repose sur plusieurs facteurs, comme la simplicité d'exécution d'une attaque ou la diversification du profil et des motifs des cybercriminels.

Il est également porté par le volume des attaques. On voit, en effet, apparaître des volumes d'attaques jusque là inégalés, que ce soit sur la couche réseau ou applicative. Lors des Jeux Olympiques de Londres en 2012, les firewall applicatifs distribués ont filtré plus de 130 milliards de requêtes qu'il a fallu analyser sans altérer la performance. Pendant les 2 premiers jours des Jeux, plusieurs attaques DDoS et des couches applicatives ont tenté de submerger les sites clés, l'une d'entre elles culminant à 11 000 règles WAF déclenchées par seconde. Pour ce type de menaces, une défense traditionnelle ne suffit plus. En effet, même si la bande passante est suffisamment dimensionnée, c'est le temps de traitement du firewall applicatif qui ralentira le service.

STRATÉGIE DE DÉFENSE

Aujourd'hui, l'intégration du cloud dans une politique globale de sécurité permet de prendre en compte ces nou-

[1] Predicts 2013: Security Solutions Gartner, 20. Nov 2012.

[2] Akamai State of the Internet Q4 2012.

Pour aller plus loin sur ITPro.fr

La protection d'accès réseau
www.itpro.fr/a/protection-acces-reseau/

Anatomie d'une attaque web
bit.ly/anatomie-attaque-web


Emmanuel Macé

> L'intégration du cloud dans une politique globale de sécurité permet de prendre en compte ces nouvelles menaces tout en gardant la souplesse d'un service, à moindre coût.

velles menaces tout en gardant la souplesse d'un service, à moindre coût. C'est dans ce contexte que de plus en plus d'entreprises se tournent vers des solutions de défense distribuée. Ce boom technologique et idéologique a permis l'apparition de nouveaux services, au-delà de la classique protection des emails via le cloud, telles que les solutions de gestion d'identité (IAM) ou de WebSecurité. Il est désormais plus facile de bloquer ou filtrer une attaque dans le cœur d'Internet que depuis l'infrastructure. Non seulement, l'infrastructure est préservée mais les utilisateurs ne sont pas impactés.

Utiliser le cloud pour se défendre est une chose, garder le contrôle de l'information en est une autre. Distribuer son système de défense ne veut pas dire mettre en place une boite noire qui va, sans aucun moyen de contrôle, faire le tri dans le trafic. Etendre son périmètre veut également dire garder la main sur les règles de protection et les informations qui remonteront de ces systèmes.

L'évolution de la sécurité du système d'information doit passer par une extension de l'infrastructure et non par la mise en place d'un nouveau composant dans le cloud. La frontière entre ces deux notions peut paraître mince mais c'est la compréhension de cette différence qui garantira le succès de la mise en place d'une telle politique.

Plus d'informations : www.akamai.com/stateoftheinternet vers le dernier rapport Akamai sur l'état des lieux d'Internet. ■

Emmanuel Macé
Solutions Engineer et Security Expert
Akamai


Olivier Clos

LA PAROLE AUX DSI

La mobilité en mode « retail »

Olivier Clos, Directeur Exécutif en charge de l'Organisation, des Systèmes d'Information et de la Supply Chain du Groupe Ludendo, nous fait part de sa réflexion sur l'évolution de la mobilité dans les magasins.

› Par Sabine Terrey

Ludendo, groupe né de son enseigne d'origine, la Grande Récré, est en train de s'étoffer, notamment grâce aux différents rachats (Hamleys, Loisirs et Création, Rue de la Fête…). « Notre métier se structure et s'élabore de plus en plus, nous sortons du domaine du pur vendeur de jouets pour arriver à l'entertainment familial » témoigne Olivier Clos. Les métiers, se multipliant à l'intérieur des magasins, créent des besoins nouveaux de mobilité (corners fête, loisirs, événementiel…). L'intérêt de la mobilité est bien réel, « il faut donc parvenir à servir correctement ces différents métiers ».

LA MOBILITÉ EN MAGASIN

« La problématique de la mobilité en magasin est un sujet évidemment essentiel pour tous les DSI travaillant dans le retail » souligne d'emblée Olivier Clos. Ce phénomène n'est pas récent car les appareils portables en magasin sont présents depuis un certain temps déjà, qu'il s'agisse de terminaux d'inventaires, de téléphones GPRS prenant des photos pour fournir la preuve par image, des smartphones sous Windows CE avec des applications de mobilité… Aujourd'hui, on assiste, néanmoins, à une vraie diversité des devices et à un progrès très fort avec l'arrivée des téléphones Android et iOS. « Nous sommes entourés d'une multitude de différents appareils ».

« Si les clients demandent de plus en plus d'assistance de la part des vendeurs, ces clients sont également de plus en plus compétents et sont surenseignés » ajoute Olivier Clos. Il faut donc armer et équiper le vendeur pour qu'il puisse apporter une vraie plus-value. Face à ce constat, des problèmes de mobilité sont posés, et il devient indispensable de fournir au directeur de magasin et au personnel des outils qui permettent de travailler plus efficacement et de mieux renseigner les clients.

DES PROJETS…

Ainsi, une première application a été développée sur iPod Touch, application permettant de faire de la preuve par image. Il faut prouver, par exemple, qu'une prestation vendue à un fournisseur (mise en avant d'une partie de la gamme pendant un laps de temps déterminé dans tel et tel

Pour aller plus loin sur ITPro.fr

Les directeurs marketing « pas encore prêts » pour le commerce mobile
bit.ly/marketing-commerce-mobile

Le e-commerce avec Commerce Server 2009 R2
bit.ly/commerce-server-2009

> La problématique de la mobilité en magasin est un sujet évidemment essentiel pour tous les DSI travaillant dans le retail.

magasin) a bien été réalisée. Cette application développée par la société Rayonnance, offre un système de prise de photos avec géolocalisation, certification du lieu et de l'horodatage de la photo, le tout en 10 mn ! Avancée majeure pour les magasins.

L'étiquetage, les tests et recherches de prix constituent le deuxième 'chantier' clé de la mobilité en magasin. Ce programme va permettre, sur des terminaux portatifs, de gérer complètement l'étiquetage et les appels prix en mobilité, d'où un gain phénoménal de temps. « Les vendeurs doivent être de plus en plus présents au côté des clients sur la surface de vente, alors que l'ordinateur se trouve souvent bien loin d'eux, ils passent leur temps en allers-retours et à l'écart des clients, ce qu'il faut absolument éviter » explique Olivier Clos. Il faut donc apporter de la mobilité au personnel en magasin pour rester au contact, tout en continuant de travailler.

Autre sujet, ce sont les éternels mails ! Le fait de donner accès aux mails aux directeurs de magasin, et aux applications d'entreprise depuis un iPod Touch ou un autre device est évidemment très positif. Ces éléments constituent des avancées concrètes et immédiatement visibles en termes d'efficacité.

Après le déploiement d'un Wifi sécurisé dans tous les magasins et de l'application de la prise de photos, le projet mail en mobilité suit, tout comme le projet étiquetage et appels prix qui sera terminé pour la fin de l'année. Très beau programme !

… EN CONCERTATION TOTALE

Des groupes de travail ont été mis en place avec des directeurs et des salariés, un responsable du réseau, un chef de projet informatique et de support. « On note ainsi une collaboration active entre le chef de projet étude et le service support sur tous les sujets, ainsi qu'un bon suivi dans la coordination du projet » commente Olivier Clos. Des magasins pilote sont choisis puis le déploiement est ensuite réalisé sur la totalité. L'avantage de l'informatique aujourd'hui est primordial : on arrive à faire des choses intuitives. Et d'ajouter « En effet, le temps sera peut-être plus long pour développer un programme, mais de l'autre côté, l'application est intuitive, simple, la prise en main se fait naturellement et très rapidement, c'est l'aspect positif ».

Quid de la sécurité ? Sur la partie Wifi (Wifi caché), des protocoles de cryptage sont installés, tout est piloté en central et passe par un firewall. Sur la partie iPod Touch, rien n'est stocké dessus, tout est stocké sur les serveurs, avec protection par mots de passe. Sur la partie étiquetage, aucune donnée n'est stockée sur les appareils. En outre, ceux-ci étant pilotés à distance, il est possible de les désactiver immédiatement, si besoin est.

DE LA MOBILITÉ EN MAGASIN AU BYOD

Quant à la question du BYOD, Olivier Clos est clair et nous livre sa réflexion sur le sujet, « Le fait que les personnes puissent récupérer leurs mails sur leurs téléphones personnels, est un bénéfice pour l'entreprise et augmente la productivité des salariés ». Sur la partie travail à domicile, les personnes sont équipées d'ordinateurs portables équipés de fonctions de sécurité validées par l'équipe IT. Par contre, le DSI refuse catégoriquement que le personnel apporte son ordinateur portable pour travailler, car la sécurité du poste n'est pas maîtrisée dans ce cas. Tout fournisseur bénéficie d'un accès Wifi spécial et sécurisé, avec une étanchéité totale par rapport au réseau, il peut se connecter aisément car la sécurité de l'accès internet fourni reste sous contrôle.

Toutefois, l'idée de se tourner vers le Client Léger (bureau à distance, TSE…) n'est pas écartée et pourra être, éventuellement, étudiée de plus près. « Mettre en place un icône (raccourci) qui pointe vers un espace du monde professionnel, le tout à distance, à partir de son ordinateur portable, semble envisageable ». Mais, pour le moment, l'infrastructure ne permet pas de choisir l'option de la virtualisation du poste de travail, ni d'ouvrir ce genre de sessions. A suivre donc… ■

L'Agora des DSI

Olivier Clos est également membre de l'Agora des DSI, club réunissant 120 directeurs de systèmes d'information de PME-PMI de plus de 500 utilisateurs.
Plus d'informations : www.agoradsi.com

SharePoint 2013 en 5 Points

> Le social, c'est l'une des briques les plus fondamentales de SharePoint 2013.

> Par Nabil Babaci

INTRODUCTION

Résumer SharePoint 2013 dans toute sa globalité est complexe. Le faire en 5 points l'est encore plus.

Dans cet article, nous allons expliquer de quelles façons cette nouvelle plateforme peut répondre à des problématiques métiers et le tout en 5 points bien évidemment.

ARCHITECTURE

L'un des premiers points et des plus fondamentaux concerne son architecture. En effet, de nombreuses modifications ont été apportées.

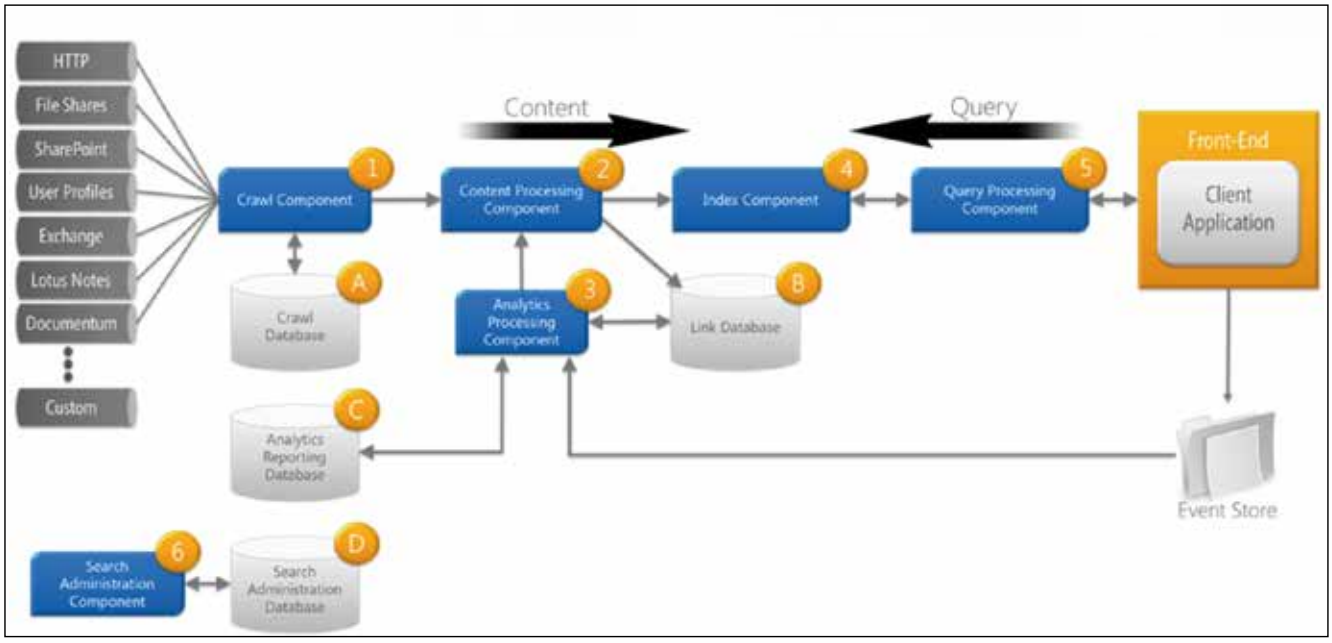


Figure 1

Pour aller plus loin sur ITPro.fr

Sharepoint 2013 : Le nouveau Facebook professionnel
bit.ly/sharepoint-facebook-professionnel

Microsoft veut casser les silos avec Yammer
bit.ly/microsoft-silos-yammer

Nouveau Framework .NET, nous passons à la version 4.5, s'ensuit un upgrade des versions de SQL Server en version 2012 et de Windows Server 2012. Au niveau de la base de données des améliorations sur la performance, le dimensionnement des tables via l'utilisation du shredded storage qui permet la compression des fichiers et améliore le trafic réseau, notamment dans l'utilisation du protocole MS-FSSHTTP (File synchronization via Soap over http).

Côté multi-tenants, cette version respecte ses engagements, nous retrouvons les mêmes fonctionnements d'une architecture multi-tenants sous SharePoint 2010, mais les changements se passent en profondeur, puisque le modèle de base de données a complètement changé, du fait de l'utilisation conjointe du moteur de Recherche.

Des nouveaux services sont apparus à savoir, un service dit « Work Management Service » qui fournit la capacité d'agrégation de tâches avec une gestion sur un point central pour l'utilisateur. Un service « Machine Translation », qui lui autorise la traduction depuis Bing, de votre contenu Word, mais aussi HTML et Texte. Et le dernier pour les « Apps Management », qui vous permettra de gérer une nouvelle fonctionnalité, à savoir les Apps. Les Apps sous SharePoint 2013, seront gérées depuis un catalogue privé. Il vous sera possible de publier vos Apps depuis un Marketplace le « SharePoint Store ».

Nous retrouvons aussi une meilleure gestion des Workflows, puisqu'aujourd'hui ceux-ci fonctionneront grâce à un Workflow Manager. Un support des Workflows depuis Azure est possible et côté SharePoint online, cela est totalement transparent pour l'utilisateur. Ce support permettra de créer des architectures hybrides mêlant On-Premise et VM Azure.

LE MOTEUR DE RECHERCHE

Dans cette nouvelle version, le moteur de recherche a complètement été revu, en vue d'offrir une robustesse suivie d'une simplicité de gestion. Ce moteur de recherche est une fusion entre FAST et Search et le multi-tenant. Ce qui implique qu'aujourd'hui nous nous retrouvons avec un modèle totalement hybride.

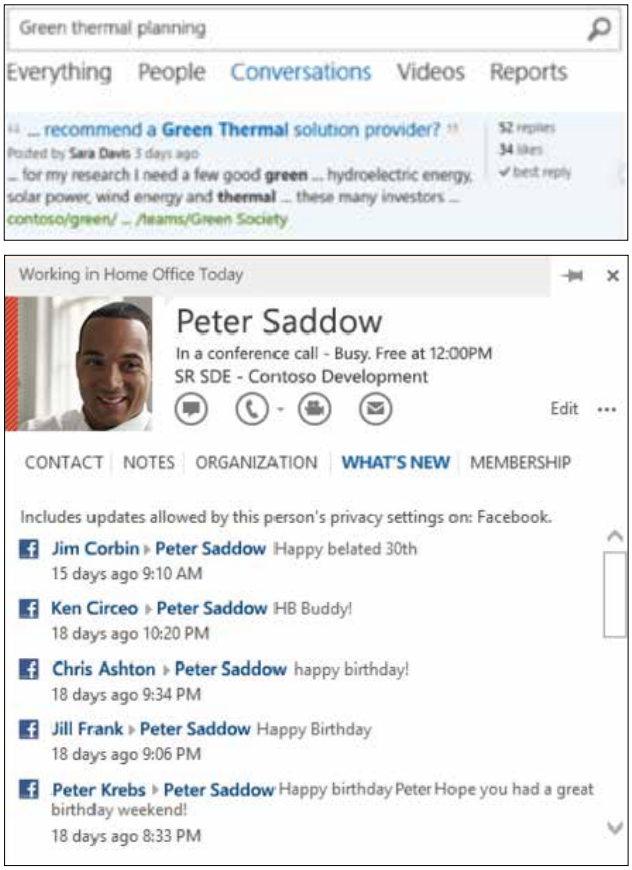


Figure 2

Voyons en détail sa description. Voir figure 1.

Connecteurs

Côté connecteurs, Search en offre un bon nombre, ceux-ci sont répartis sous 2 formes. La première appelée « Protocol Handler » prenant en compte les points suivants : tout contenu provenant de SharePoint, les Files Share, WebSite et la couche People. Le deuxième connecteur « BCS Connector » est un peu spécial. Par défaut, nous retrouvons la prise en charge de Lotus Notes, EMC Documentum, un connecteur Taxonomique et des Dossiers publics d'Exchange, mais vous avez aussi la possibilité de créer des solutions de connexion personnalisées en exploitant le Framework BCS. Ainsi, ces données peuvent provenir d'une base de données, de service WCF ou de développement .Net.

Composants

Côté composants, les détailler tous prendrait beaucoup de temps, mais dans les grandes lignes nous retrouvons :

- Le Crawl.
- Traitement de Contenu.
- Traitement d'Analyse.
- Les Index.
- Traitement des requêtes.
- Composant d'administration.

Figure 3 : La fenêtre des Codes Snippet

Haute disponibilité

Le nouveau moteur de Search s'est doté de mécanisme de haute disponibilité hérité de FAST. En effet, il vous sera possible, en fonction de votre architecture, d'utiliser les possibilités de « Répartition des index primaires et/ou secondaires » sur vos serveurs. Et ainsi, bénéficier d'une répartition de la charge des requêtes mais aussi des ressources consommées.

Display Template

Outre son nouveau modèle architectural, la recherche a, elle aussi, subi un rafraîchissement puisqu'elle autorise l'utilisation du HTML, CSS et JS pour transformer le visuel de recherche (Display Template) et ainsi offrir un confort de développement. Ajoutons que des nouvelles Web Parts de recherche font leur apparition.

LE SOCIAL

C'est l'une des briques les plus fondamentales de SharePoint 2013. La brique Sociale a subi un lifting. L'utilisateur est centre de tout. En effet, l'idée principale est très fortement axée sur la communication. Le mode de communication a été emprunté aux Facebook et autre Twitter du genre.

Côté MySites

Voici ce que nous pouvons retrouver sur les MySites :

- Fonctionnalité de MicroBlogging.
- Les likes.
- Les hastag et mentions.
- Les tendances.
- La possibilité de suivre des personnes, des documents, des sites.
- Ses propres Apps.
- Ses propres Tâches.

Côté Communautaire

La partie communautaire a, elle aussi, subi des changements :

- Des sites Communautaires.
- Un Processus de récompenses des membres les plus actifs (badges).
- Un portail Communautaire recensant l'ensemble des sites communautaires.

Yammer

Notons aussi l'arrivée de Yammer pour une cible plus Online (Office 365). Yammer est un outil de MicroBlogging pour Entreprise ou pour Communauté. Celle-ci peut être couplée à SharePoint On-Premise au travers d'une WebPart pour remplacer le Newsfeed. Nous retrouvons les fonctionnalités communes à toute plateforme de RSE, à laquelle s'ajoutent des applications mobile et desktop.

D'un point de vue plus macro, nous pouvons distinguer 3 points fondamentaux :

- NewsFeed Hub: C'est le point central à toute communication, avec une capacité de partager du contenu selon une cible dédiée, de suivre des personnes, de « tagguer » des personnes.
- Skydrive Hub: Devient l'espace de stockage des documents et autres photos des profils. Vous retrouvez aussi les documents suggérés.
- Sites Hub : Points d'entrée aux sites communautaires, ceux qui sont suggérés et ceux que vous suivez.

La Recherche Sociale

Etant donné que l'utilisateur est au centre de tout, il appa-

rait tout naturellement que celui-ci se retrouve aussi dans la recherche. Vous aurez aussi la possibilité de faire des recherches sur l'ensemble des conversations. Mais aussi d'afficher son profil, grâce un survol, d'afficher ses données, de communiquer avec lui au travers de Lync 2013 et de lui envoyer des mails soit sur boîtes aux lettres perso ou via une boîte aux lettres de Site « Site Mail box ». Voir figure 2.

DESIGN

La partie Design sous SharePoint 2013 a complètement été revue, aussi bien sur l'interface que sur son mode de management. Ainsi, nous disposons aujourd'hui d'une interface basée entièrement sur HTML 5 et CSS 3. Ajouté à cela que maintenant un gestionnaire de Design, le « Designer Manager » a été implémenté.

Ce Designer Manager permet aux utilisateurs, dont la cible peut être les designers, les développeurs ou utilisateurs finaux, de créer des packages de templates en ayant la possibilité de les publier soit sur une plateforme On-Premise ou Online, et tout cela en seulement quelques clics, autrement dit une vraie révolution. Toujours dans le Designer Manager, une avancée majeure est la partie relative aux « Code Snippet », qui permet d'avoir une vue d'ensemble des fonctionnalités SharePoint, de les intégrer par un simple copier-coller et de voir son résultat immédiatement via la prévisualisation.

Plus simplement, nous retrouvons une gestion des thèmes de site, anciennement les Thèmes faits sous PowerPoint (.Thmx), beaucoup plus simplifiée. Notons toutefois que l'utilisation du Designer Manager ne peut se faire que sur la brique Web Content Management (Publishing).

Une des fonctionnalités fortement utilisées, concerne l'utilisation des canaux de périphériques « Device Channels » qui permettent en quelques clics de configurer notre site internet pour n'importe tablette, smartphone ou encore navigateur. Voir figure 3.

Un dernier point consiste dans la navigation des pages, puisque dorénavant, celle-ci possède en plus une navigation pouvant se basant sur la Taxonomie. Ainsi, cela rend un usage plus simple et plus centralisé des pages. Mais aussi, une utilisation plus en adéquation avec les mécanismes relatifs à la SEO.

BUSINESS INTELLIGENCE, COMPOSITE

Dernier point, mais certes il y en aura toujours et ce car la technologie est vraiment vaste, concerne l'utilisation de la couche BI et Composite sur SharePoint. Dans la brique Composite, nous retrouvons essentiellement l'utilisation de Business Connectivity Service.

Cette fonctionnalité qui permet d'ajouter du contenu externe à votre plateforme et de le rapatrier en tant que donnée externe, possède maintenant pléthore de nouveautés. Nous retrouvons la capacité de se connecter à une source de données provenant soit de développement .Net, de service WCF, d'une base SQL ou SQL Azure et de consommer des services ODATA.

Autrement dit un outil parfait pour l'intégration de vos composants Line of Business (LOB).

Ajoutons que la consommation de ces données se fait sur la plateforme SharePoint mais peut aussi se faire côté client, avec l'utilisation d'Office 2013, ainsi Word, Excel, Access, Visio, InfoPath et Outlook et peut fonctionner indépendamment de SharePoint.

Lorsque l'on parle de BI sous SharePoint, on doit parler « Ecosystème ». En effet, cela implique les briques relatives à SQL Server 2012 en l'occurrence :

- SQL Server Reporting Service.
- SQL Server Integration Service.
- SQL Server Analyse Service.

A cela, s'ajoutent les briques Power Pivot (amélioration du moteur) et Power View qui vous permettent de consommer et de visualiser de la BI de façon plus utilisatrice et plus simplifiée. Excel Services qui vous permet de consommer de la BI dans SharePoint, via maintenant le navigateur.

Performance Point Service existe toujours et possède de nouvelles fonctionnalités telles que la migration du Dashboard, un meilleur support pour tablettes notamment IPAD. Nous retrouvons aussi un template de BI dédié.

En conclusion, nous pouvons dire que SharePoint 2013 possède toutes les qualités requises pour faire soit de la BI, soit des sites Internet, des applications composites ou des architectures hybrides ou encore faire le grand saut totalement vers le Cloud. ■

Nabil Babaci
MVP SharePoint

L'activité économique s'accélère sans cesse et il devient plus difficile de garder le rythme. Il suffit d'une pause pour se faire distancer.Pour rester en tête, vous devez exploiter la moindre parcelle de productivité dans tous les départements. Mais, il n'est pas seulement question de technologie.

Il faut optimiser les ressources humaines en leur proposant les outils adaptés pour aller encore plus loin. C'est pourquoi plus de 90 % des sociétés du classement Fortune 1000 choisissent les produits ultraperformants de Condusiv™ Technologies. Quelle stratégie allez-vous adopter pour suivre le rythme toujours plus soutenu de l'activité économique ?

Pour découvrir comment Condusiv peut vous aider à penser plus rapidement, visitez notre site Web Condusiv.com ou appelez le **+44 1342 821 334**

Diskeeper is now

Condusiv Technologies

V-locity® | Diskeeper® | Undelete® | ExpressCache®


Arnaud Alcabez

CLOUD IT EXPERT

Le monde au bout des doigts

› Par Arnaud Alcabez

Si Dieu a fait l'homme à son image, Il ne l'a toutefois pas doté des mêmes capacités, fort heureusement, car cela fait longtemps que nous aurions déjà pulvérisé notre planète.

Néanmoins, l'homme n'a de cesse de contrôler son environnement, quitte à inventer les outils les plus extraordinaires pour pallier ses défauts et ses handicaps naturels. Ainsi, créer le feu ou obtenir de la lumière sur commande, voler comme un oiseau, plonger à des profondeurs où la pression nous écraserait comme une vulgaire canette de soda en aluminium, remplacer des parties de notre corps endommagé par des prothèses, ou partir dans l'espace font partie de notre quotidien ou presque[1].

Télépathie, télékinésie, don d'ubiquité, et omniscience sont des capacités que nous possèderons dès demain. L'omnipotence quant à elle sera toutefois encore limitée quelques années avant que tous les objets de notre environnement disposent d'un identifiant unique, comme une adresse IP ou un tag ID NFC.

Vous trouverez un bon exemple de vos futures aptitudes télékinésiques en découvrant cette petite vidéo : http://www.youtube.com/watch?v=oWu9TFJjHaM

On peut donc recomposer notre environnement informatique de demain en bulles, de celle de proximité immédiate (quelques centimètres) à celle la plus distante pouvant être située à plusieurs dizaines de milliers de kilomètres, pour définir une nouvelle vision du système numérique avec lequel nous interagirons (figure 1).

› Télépathie, télékinésie, don d'ubiquité, et omniscience sont des capacités que nous possèderons dès demain.

La bulle de proximité immédiate et confidentielle demande la présence physique, sans toutefois nécessiter de contact avec l'objet. C'est par exemple le cas pour le paiement de proximité, verrouiller ou déverrouiller les portières de votre véhicule ou le démarrer. La technologie la plus adaptée étant le NFC (Near Field Communication ou en français Communication en champ proche)[2].

La bulle personnelle correspond à un périmètre limité de quelques mètres, c'est-à-dire dans un espace dans lequel peut encore porter votre regard. Ponctuellement, vous pouvez être amené à accepter un nombre restreint et connu d'objets connectés de tiers à condition d'être mutuellement approuvés. La technologie la plus adaptée étant le Bluetooth, utilisé pour les Google Glass, les bracelets Myo, et d'autres dispositifs qui vous sont proches et situés à une dizaine de mètres maximum[3].

[1] http://fr.wikipedia.org/wiki/Tourisme_spatial
[2] http://fr.wikipedia.org/wiki/Communication_en_champ_proche
[3] http://fr.wikipedia.org/wiki/Bluetooth

Pour aller plus loin sur ITPro.fr

Les ordinateurs bientôt dotés des cinq sens
bit.ly/ordinateurs-cinq-sens

L'informatique contrôlée par la pensée
bit.ly/leweb-internet-objets

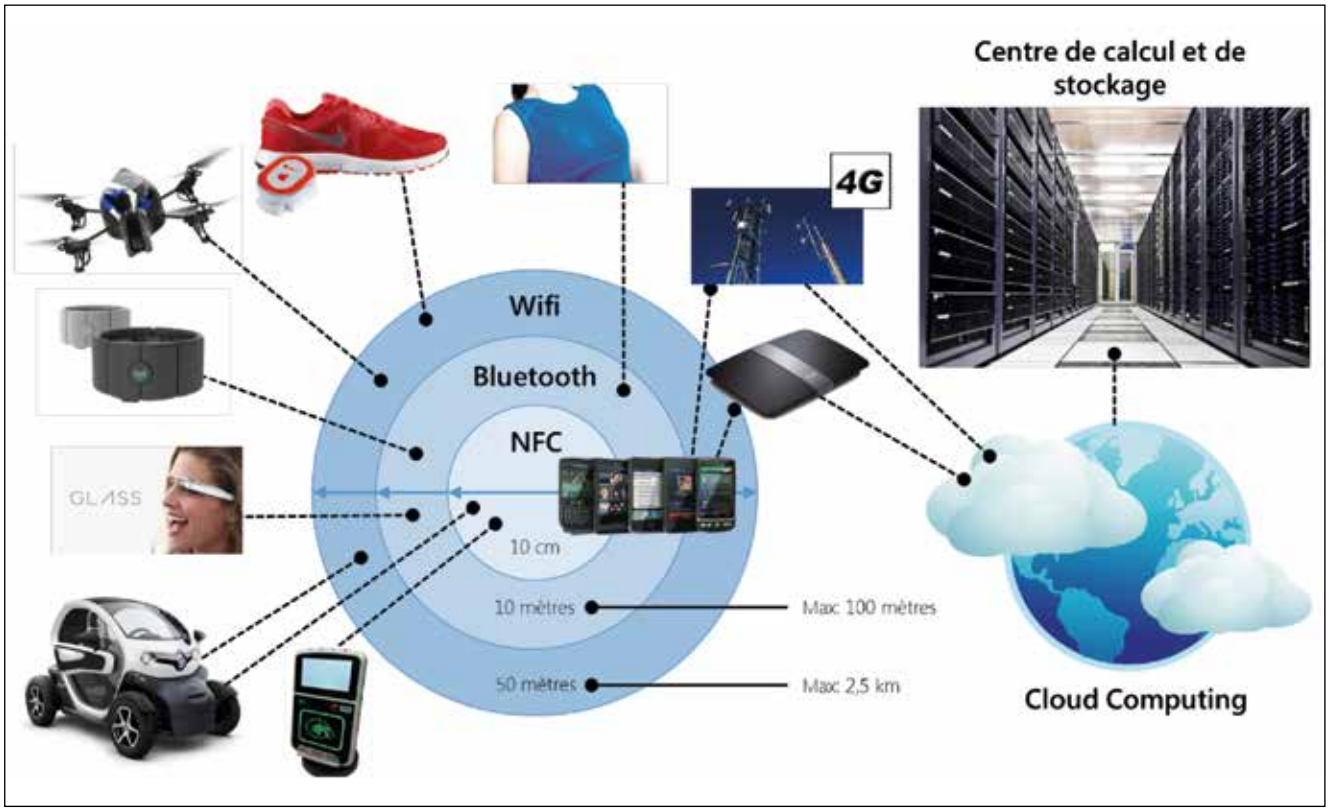


Figure 1 : De bas en haut dans le sens des aiguilles d'une montre: Lecteur NFC pour le paiement sans contact, Renault Twizy, Google Glass, bracelets Thalmic Myo, Parrot AR Drone, kit Nike+iPod, Smart textiles, pouvant être biométriques, à traitement médical ou simplement changer de couleur en fonction de l'environnement. Toutes les technologies représentées ici sont soit déjà disponibles, soit le seront d'ici quelques mois.

La bulle personnelle augmentée ou de partage domestique, soit un périmètre d'une cinquantaine de mètres, qui permet de communiquer avec des dispositifs hors de votre champ de vision, comme un drone AR Parrot, une imprimante, les éléments de sécurité de votre maison, ou votre routeur Internet. La technologie la plus adaptée étant le Wifi[4].

Le smartphone devenu un hub intelligent pour la communication entre les dispositifs connectés des différentes bulles et également utilisé comme client d'accès à Internet. Doté de 4 Go à 64 Go RAM, de 1 à 4 cœurs processeurs, il permet un traitement rapide des données, mais limité en termes de puissance de calcul et de stockage.

Le Cloud Computing, lorsque la puissance du smartphone n'est pas suffisante, permet de faire appel un traitement massif, non limité en puissance que ce soit en RAM, en cœurs processeurs ou en I/O, ou impliquant un nombre de composants ou d'individus multiples, tels la Business Intelligence, la cartographie, les échanges entre utilisateurs distants, l'accès au stockage, le traitement du signal, qu'il soit audio ou vidéo.

L'environnement étendu, enfin, se situant au-delà de notre sphère personnelle, à l'autre extrémité du réseau Internet. Il nous permet de communiquer sur l'ensemble des nœuds du réseau pour joindre les objets communicants et interagir avec eux quelle que soit leur position sur le globe.

Demain, donc, animer les objets par notre simple présence, les piloter d'un geste de la main, communiquer avec n'importe quelle personne ou groupe de personnes en simultané sur la planète, tout en ayant un accès immédiat à la connaissance à la simple présence dans un lieu ou d'un regard sur un objet, deviendront si évidents que les générations futures se demanderont comme nous avons fait pour (sur)vivre sans jusqu'alors. ■

Arnaud Alcabez
MVP Office 365
Enterprise Architect, Capgemini

[4] http://fr.wikipedia.org/wiki/Wifi

Loïc Thobois

Mise en place de Hyper-V Replica

› Par Loïc Thobois

Ce mois-ci, nous allons nous attarder sur la fonctionnalité Hyper-V Replica qui permet de mettre en place un PRA nativement et facilement dans Windows Server 2012 et ceci sans surcoût.

L'objectif de la technologie Hyper-V Replica est de permettre la réplication asynchrone, à chaud, des disques durs d'une machine virtuelle entre deux hyperviseurs afin de pouvoir basculer l'exécution de la machine virtuelle sur un site distant lorsque cela est nécessaire.

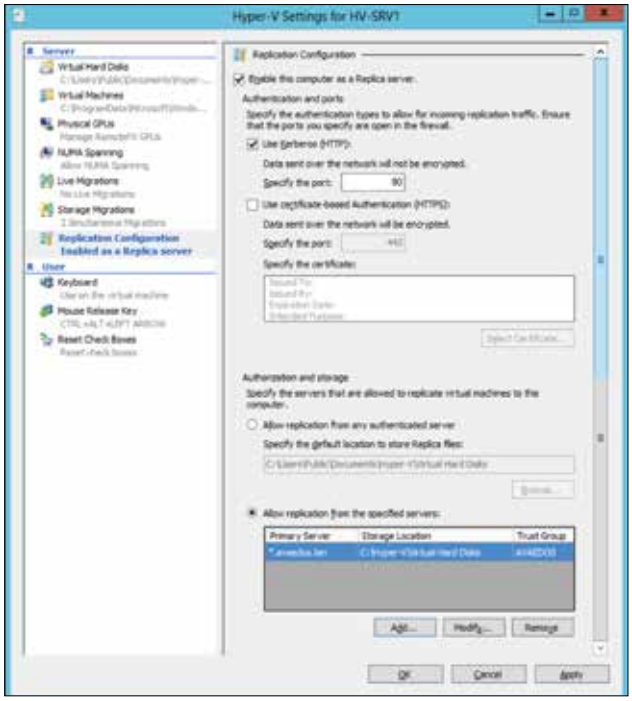


Figure 1

Seule une connectivité IP sur le port TCP 80 (HTTP) ou sur le port TCP 443 (HTTPS) est nécessaire sur l'infrastructure réseau pour transférer les données entre les serveurs. Les modes de communication utilisables ainsi que leur configuration vont être spécifiés directement dans les paramètres de chaque serveur Hyper-V voulant répliquer. Voir figure 1.

L'avantage d'utiliser les protocoles HTTP et HTTPS est qu'ils ne posent pas de souci particulier avec les pare-feu qui les laissent souvent passer.

Lorsque le protocole HTTP sera choisi, le composant de réplication va s'appuyer sur le protocole Kerberos pour assurer l'authentification des serveurs ce qui oblige les serveurs Hyper-V à être membres d'un domaine Active Directory.

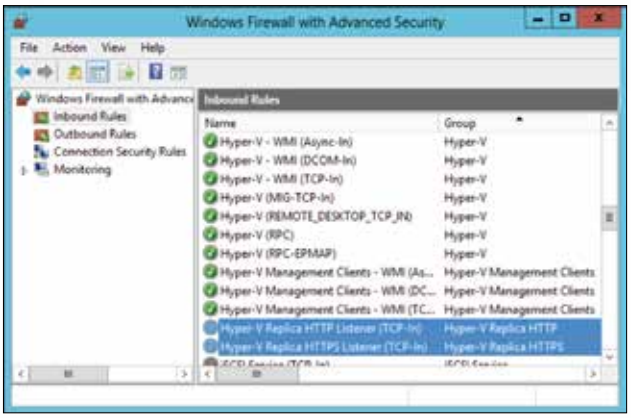


Figure 2

Pour aller plus loin sur ITPro.fr

Hyper-V Replica
www.itpro.fr/a/hyper-v-replica/

Les nouvelles fonctionnalités d'Hyper-V avec Windows Server 2012
bit.ly/nouvelles-fonctionnalites-hyper-v

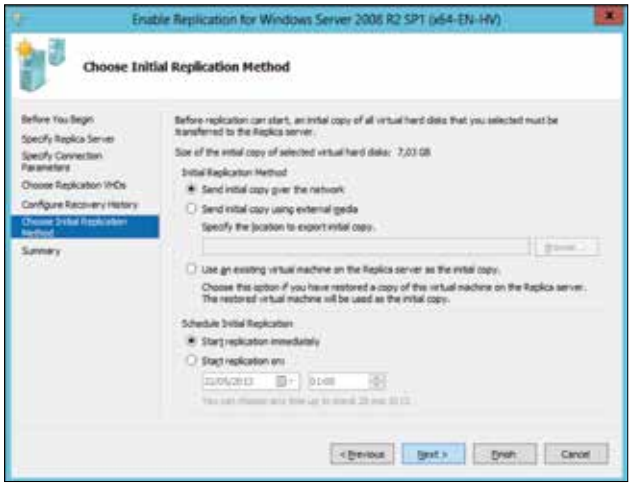


Figure 3

Si l'on choisit d'utiliser le protocole HTTPS comme protocole de transport des données, il est alors nécessaire d'implémenter ou d'utiliser une autorité de certification afin de générer les certificats garants de l'authentification de chacun des serveurs. Cette solution, ayant une implémentation plus complexe, permet de mettre en place la réplication entre des machines hors domaine ou n'étant pas membres du même domaine.

Des groupes de serveurs approuvés seront ensuite spécifiés grâce à une identification FQDN et à un tag d'approbation (simple chaîne de caractères).

Une fois la configuration mise en place, il faudra valider que les règles du pare-feu des serveurs répliquant ensemble autorisent le protocole choisi. Pour cela, des règles prédéfinies sont présentes dans l'outil pare-feu de Windows Server 2012 qu'il suffit d'activer. Voir figure 2.

Une fois la configuration des serveurs finie, il sera nécessaire de configurer individuellement chaque machine virtuelle devant être répliquée. Pour cela, il suffit de d'utiliser l'option Réplication du menu contextuel sur la machine virtuelle et de compléter les informations suivantes demandées par l'assistant :

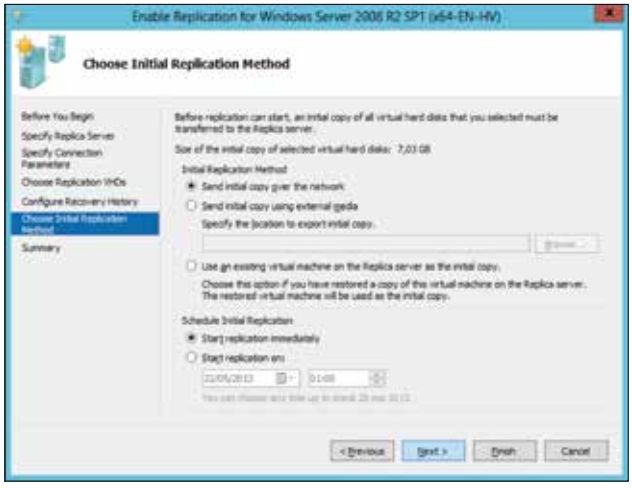


Figure 4

Figure 5

Figure 6

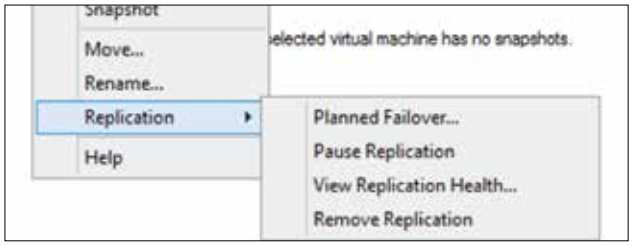


Figure 7

- Le nom du serveur accueillant la copie de la machine virtuelle.
- Le port et la technologie choisie pour la réplication selon la disponibilité sur le serveur ainsi que les paramètres de compression des données (charge supplémentaire nécessaire pour réaliser la compression-décompression).
- La liste des disques attachés à la machine qui seront répliqués.
- L'historique des versions de la machine qui seront maintenues sur le réplica permettant de restaurer la machine dans un état précédent. Ceci est mis en place par l'intermédiaire de snapshot. Voir figure 3.
- La méthode et la planification de la réplication initiale de la machine virtuelle, voir figure 4.

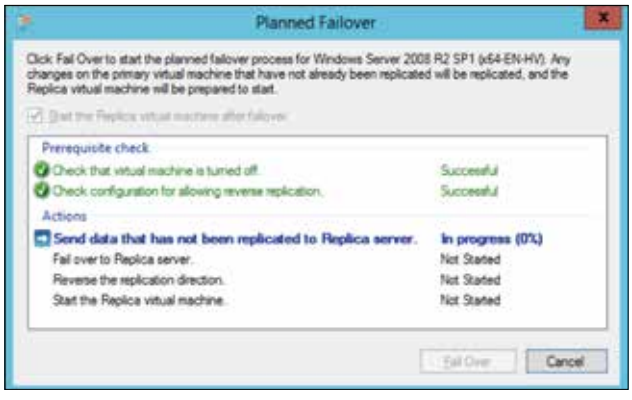


Figure 8

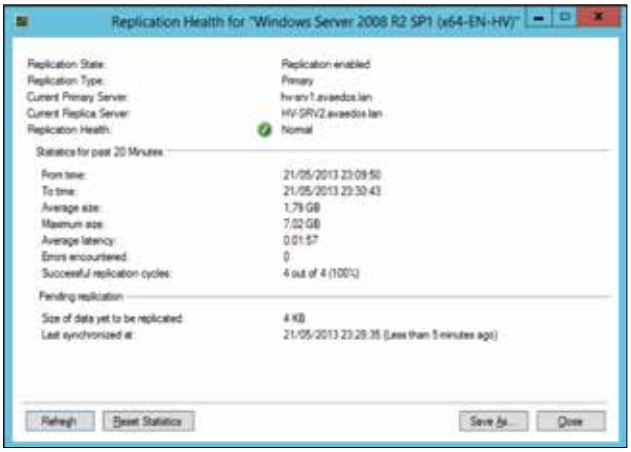


Figure 9

Des commandes PowerShell permettent d'automatiser ces tâches si nécessaires :

- Enable-VMReplication
- Get-VMReplication
- Get-VMReplicationAuthorizationEntry
- Get-VMReplicationServer
- Import-VMInitialReplication
- Measure-VMReplication
- New-VMReplicationAuthorizationEntry
- Remove-VMReplication
- Remove-VMReplicationAuthorizationEntry
- Reset-VMReplicationStatistics
- Resume-VMReplication
- Set-VMReplication
- Set-VMReplicationAuthorizationEntry
- Set-VMReplicationServer
- Start-VMInitialReplication
- Stop-VMInitialReplication
- Stop-VMReplication
- Suspend-VMReplication
- Test-VMReplicationConnection

Les machines vont ensuite passer par plusieurs états pour la mise en place de la synchronisation: voir figures 5 et 6.

Une fois la synchronisation établie, plusieurs options d'administration sont disponibles sur les serveurs via un menu spécifique.

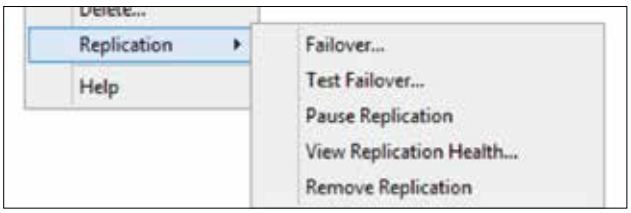


Figure 10

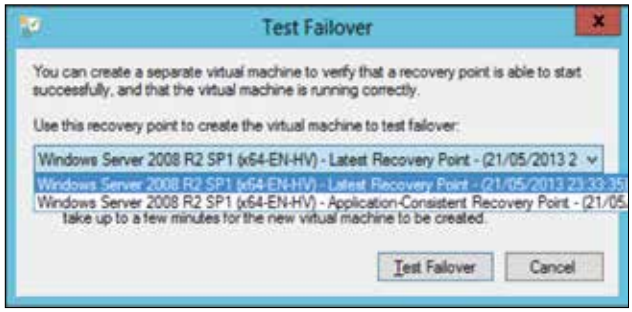


Figure 11

Ainsi, l'on va retrouver les opérations suivantes sur le serveur détenant l'image source : voir figure 7.

- La planification d'un basculement qui nécessite que la machine virtuelle soit arrêtée et qui va synchroniser les disques pour la redémarrer sur le serveur distant et inverser automatiquement le sens de synchronisation.Voir figure 8.
- Mettre en pause la réplication.
- Voir l'état de santé de la réplication de la machine, voir figure 9.
- La suppression de la réplication.

Sur le serveur détenant le serveur de destination, on va retrouver spécifiquement les deux opérations suivantes: voir figure 10.

- L'option de basculement qui sera l'option à lancer uniquement si le serveur et l'image virtuelle source sont défaillants. Cela va permettre de rendre active la copie en lieu et place de la source. L'assistant vérifie en amont que la machine d'origine est bien éteinte ou indisponible. Il est possible de choisir la « version » de la machine virtuelle parmi l'historique qui a été maintenu lors de la réplication.
- L'option de test de basculement qui va créer une machine virtuelle dans l'état de réplication, choisit afin de valider le bon fonctionnement et la capacité à remettre en production la machine si nécessaire. Là encore, il est possible de choisir la « version » voulue. Cette opération n'interrompt pas le processus de réplication en cours. Il est à noter que la suppression de cette machine est automatisée par une option spécifique. Voir figure 11.

Dans les propriétés de la machine virtuelle, on trouvera pour finir, les paramètres de la stratégie de réplication, nous permettant de les modifier a posteriori. ■

Loïc Thobois
Consultant, Formateur et Administrateur de la plate-forme de partage communautaire www.avaedos.com.
MVP depuis 7 ans, il est passionné des technologies Microsoft et partage ses connaissances sur ce sujet depuis plus de 10 ans.

La référence des magazines informatiques professionnels. Des ressources exclusives aux services de vos compétences et de celles de vos équipes.

IT Pro Magazine N° ISSN 1961 - 3814

1er mensuel dédié à la gestion et l'optimisation des environnements Windows d'entreprise, des infrastructures virtualisées, du Cloud Computing, des solutions de messagerie, collaboration et mobilité d'entreprise.

10 numéros par an : 95 € TTC

1ère publication technologique dédiée aux professionnels des environnements Windows Server, des infrastructures virtualisées, de Cloud Computing. IT Pro Magazine s'enrichit des dossiers Exchange Magazine dédiés à la gestion des solutions de messagerie, collaboration et solutions mobiles d'entreprise. La nouvelle formule enrichie du mensuel IT Pro Magazine constitue un formidable support d'informations technologiques et stratégiques pour accompagner vos compétences et vous permettre de tirer le meilleur profit de vos environnements informatiques d'entreprise.

Les Dossiers Exchange Magazine

L'expertise technologique et stratégique pour la gestion des environnements de messagerie, de collaboration et les services mobiles d'entreprise.

Les dossiers et ressources informatiques pour la compréhension, la gestion et l'optimisation des environnements de messagerie, des plateformes collaboratives et solutions mobiles d'entreprise. Une ligne éditoriale à forte vocation technologique et une dimension stratégique unique, signée des meilleurs experts français et internationaux. Bénéficiez d'un véritable concentré d'expertise pour vous accompagner dans la mise en place, la gestion et l'optimisation des nouvelles solutions de collaboration étendue d'entreprise.

Le Club Abonnés sur iTPro.fr !

Des services exclusifs, réservés aux abonnés des magazines !

Le Club Abonnés regroupe des services exclusivement réservés aux abonnés, c'est un service inclus dans votre abonnement et un complément indissociable des magazines. Le Club Abonnés est disponible dans une rubrique dédiée sur le site www.iTPro.fr. Il vous donne accès à l'intégralité des archives des magazines, au format .PDF soit près de 1800 dossiers publiés depuis 2002 avec tous les scripts, codes et autres exécutables qui complètent chaque mois les dossiers publiés dans IT Pro Magazine, System iNEWS et Exchange Magazine.

Avis d'experts & Ressources IT stratégiques

Les dossiers informatiques stratégiques pour comprendre les enjeux mais aussi les perspectives associées aux nouveaux usages et la valeur de la mise en œuvre des services informatiques de nouvelle génération.

Les fils éditoriaux stratégiques pour les responsables informatiques en charge d'assurer la pérennité et l'effectivité des environnements et des services informatiques dont ils ont la responsabilité. Les avis d'experts & les ressources IT stratégiques publiés dans IT Pro Magazine sont des dossiers exclusifs, des points de vue, des chroniques, signés des journalistes, experts et contributeurs reconnus de l'informatique d'entreprise.

OFFRE D'ABONNEMENT SIMPLE	France	Etranger
☐ IT Pro Magazine 1 an soit 10 N°+ Club abonnés	95 € TTC*	119 € HT**
+ Les dossiers Exchange Magazine & les dossiers SQL Server Magazine		

L'abonnement principal concerne :

Société _____

Nom du contact _____

Adresse de livraison _____

Code postal _____ Ville _____ Pays _____

Tél. : _____ Fax : _____

Adresse de facturation (si différente de l'adresse de livraison) _____

_____

OFFRE D'ABONNEMENT DUO	France	Etranger
Je choisis d'abonner une 2ème personne au sein de la société en plus de l'abonnement principal		
☐ IT Pro Magazine 1 an soit 2x 10 N°+ Club abonnés	142,50 € TTC*	192 € HT**
+ Les dossiers Exchange Magazine & les dossiers SQL Server Magazine	~~190 € TTC~~	~~238 € TTC~~

Le second abonnement concerne :

Société _____

Nom du contact _____

Adresse de livraison _____

Code postal _____ Ville _____ Pays _____

Tél. : _____ Fax : _____

*France : TVA 19,6%

** Taux de TVA du pays destinataire/surtaxe postale incluse soit 27 € par titre

MODE DE RÈGLEMENT

☐ A réception de facture : réservé aux sociétés en france - Belgique - Luxembourg - Suisse

☐ Par chèque joint

☐ virement bancaire

Indiquez votre N° IVA : _____

Références bancaires BNP :

Code Banque	Code guichet	Numéro de compte	Clé rib
30004	02953	00010009051	61

IBAN International Bank Account Number
FR 76 3000 4029 5300 0100 0905 161

BIC Bank Identification Code
BNPAFRPPLAY

Signature (obligatoire)

Renvoyez votre bulletin à notre service abonnements

IT MEDIA - Service Abonnements
BP 40002 - 78104 Saint Germain en Laye cedex
Fax +33 1 39 04 25 05 - E-mail : abonnement@itpro.fr


Eudes-Olivier Robert


Olivier Gerling

INFRASTRUCTURE IT EXPERT

Un grand changement dans les services d'infrastructures

› Par Eudes-Olivier Robert et Olivier Gerling

Aujourd'hui, les services d'infrastructures s'adaptent aux usages qui ont été lancés dans les services mobiles.

Dans les années 2000, arrivent les téléphones intelligents appelés « Smartphones » avec Windows mobile et puis iPhone. Apple a démocratisé ce que l'on appelle les centres de téléchargement d'applications dématérialisées, aussi connus sous le terme de « Application Store », ce fut une révolution dans les usages, et aujourd'hui, ce qui a fait le succès de la marque à la pomme, a permis de faire basculer le monde du mobile : il y a plus de smartphones vendus dans le monde que de téléphones mobiles traditionnels. Tous les constructeurs ont leur store. Mais tout cela n'est pas si loin : le lancement de l'Apple Store a eu lieu le 11 juillet 2008.

Cet usage des Stores s'est ensuite déporté dans le monde des ordinateurs personnels avec Apple encore, qui l'a lancé sur ses MacBook, puis sont arrivés les stores dédiés tablettes, les stores sur Box opérateur avec un précurseur français : Free et sa Freebox, les constructeurs de TV Connectée, les constructeurs de consoles de jeu type XBOX et même les constructeurs de matériels réseau dédiés comme SONUS avec un store sur ses « sessions managers ». Aujourd'hui, ces services arrivent sur les téléphones fixes avec le constructeur allemand Snom.

Tous ces stores sont une nouvelle manière d'enrichir l'expérience utilisateur, répondant et développant de nouveaux usages sur mesure avec des applications innovantes.

Une installation d'application qui peut paraître lente, fatigante, truffée de publicité, perdue au milieu d'informations polluantes, voire même parfois perturbantes, devient simple et facile.

A quoi bon lancer un navigateur web, taper une adresse, lancer une recherche, trier les résultats de cette recherche, passer par 3 ou 4 écrans différents pour enfin obtenir le lien de téléchargement, choisir le répertoire de téléchargement puis subir une longue installation QUAND on peut ouvrir l'application store, effectuer sa recherche et installer directement !

Depuis l'émergence des stores, les développeurs, riches de leurs expériences, chacun dans leurs domaines, nous ravissent de leur créativité à améliorer l'utilisation de nos appareils.

Pour aller plus loin sur ITPro.fr

Dossier SIP
www.itpro.fr/t/sip

Comment intégrer un MDM dans votre entreprise ?
bit.ly/integrer-mdm-entreprise

Ils sont le complément essentiel des appareils développés par les constructeurs et l'adaptation de leurs usages.

A cet effet, snom technology AG, pionnier des téléphones basés sur le protocole ouvert SIP, annonce un grand concours «Les pionniers du snom APPPOINT», du 10 Avril 2013 au 30 Juin 2013 Minuit. Ce concours servira au lancement du Store « snom APPPOINT » dédié aux postes Snom début juillet 2013.

A travers ce concours, snom souhaite encourager le développement des nouvelles exigences des usages de la téléphonie sur IP : permettre d'enrichir le poste d'application, apporter une vrai différence entre la téléphonie IP et le traditionnel, être plus productif, connecté à ses environnements de travail, et à sa communauté…

snom a développé de nombreuses fonctionnalités dans ses téléphone SIP, dont certaines qui permettent au téléphone de s'interconnecter à différents environnement systèmes (applications logiciel…), à des services Cloud, à l'environnement réseau (caméra IP, portier…), connexion en Wifi et bien plus. Les développeurs pourront créer des idées d'applications infinies et vont faire émerger des projets très intéressants et applicables rapidement dans le milieu de l'entreprise. ■

Rejoignez-nous et participez à snom APPPOINT : http://apppoint.snom.com

Eudes-Olivier Robert
MVP Lync
Professional Services chez NextiraOne

Olivier Gerling
Managing director for Snom France

Déployer Lync 2013 selon la méthode du PMI

Quelle place pour le télétravail dans un environnement hyper connecté et mobile ?

› Par Cécile Coste et Laurent Teruin

Lync 2013 ! Voilà un outil Microsoft qui rend la vie plus belle à nombre de professionnels et d'entreprises. En effet, cette nouvelle plateforme de communications unifiées permet de connecter des millions d'utilisateurs, où qu'ils soient, en direct, en images et en groupe ! Cette souplesse, avec le partage de contenu, améliore bien sûr l'efficacité de chacun et la productivité de tous mais au-delà, Lync 2013 modifie la manière d'appréhender un dossier, de développer des projets. On peut comprendre alors que les entreprises et leurs dirigeants envisagent la migration de leurs systèmes et de leurs équipes vers Lync 2013. Et c'est là que le choix de la méthode d'intégration de ce projet au sein de l'entreprise, et auprès des utilisateurs finaux, est crucial. Et la professionnalisation de la gestion de projet prend tout son sens à l'ère de la globalisation d'une communication sans frontière !

Méthode Agile, en V, Meurise ou tout autre modèle, les solutions sont multiples.

Mais rappelons que seulement 2 % des logiciels livrés fonctionnent à la livraison et que 20 % d'entre eux seront utilisés après des modifications majeures (source Congrès américain 2000). C'est donc pourquoi, nous vous proposons ici d'aborder l'intégration de Lync 2013 dans le cadre de la méthode PMP du Project Management Institute. Car cette logique de gestion de projet est de plus en plus utilisée, notamment en Europe, pour les nombreuses qualités qu'elle comporte. En effet, les gestionnaires de projet apprécient aujourd'hui de travailler avec une approche multidisciplinaire, tenant ainsi compte, autant des connaissances techniques existantes que des connaissances

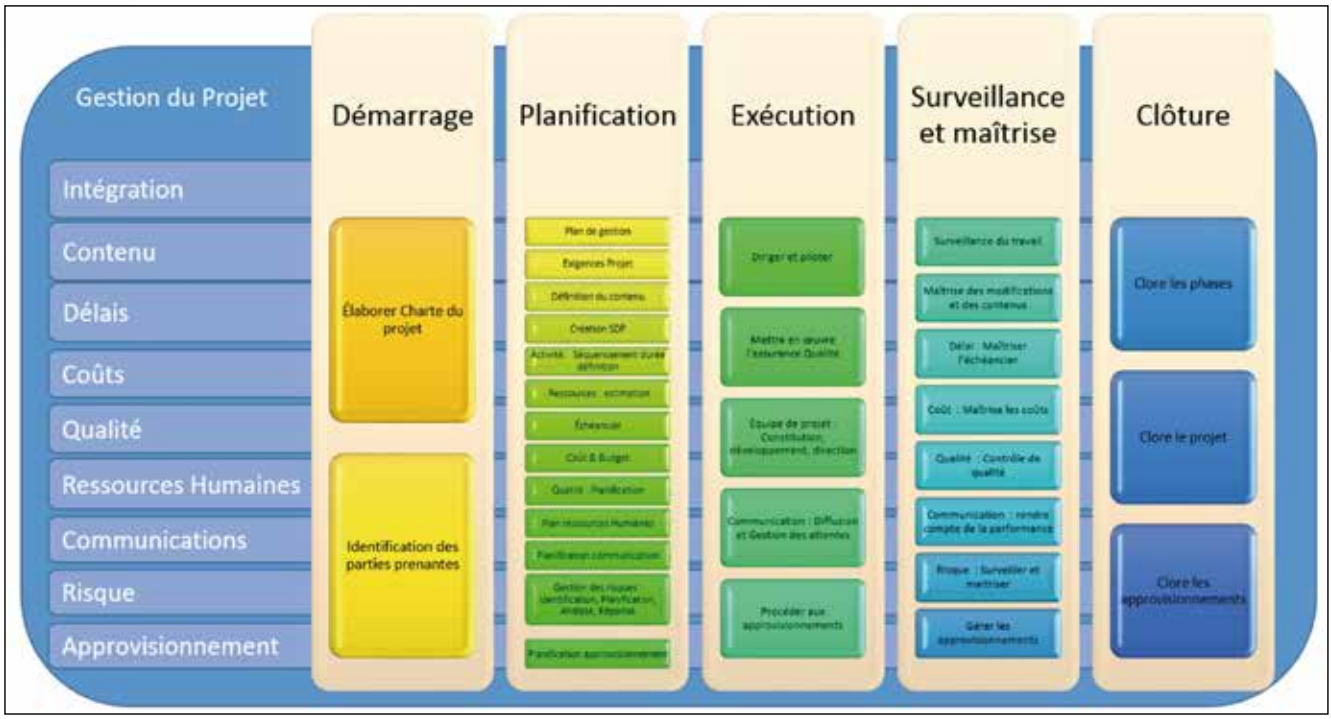


Figure 1

Pour aller plus loin sur ITPro.fr

Dossier Lync Server
www.itpro.fr/t/lync

Les annonces de la Lync Conference
bit.ly/lync-conference

spécifiques au milieu propre à chaque projet, en utilisant bien sûr les ressources de gestion disponibles.

La volonté d'appréhension globale du projet par cette méthode PMP répond ainsi à des besoins modernes, tout en apportant une structuration de chaque aspect par groupe de processus. Et cette formalisation, dès qu'elle est maîtrisée, peut permettre d'éviter de nombreux écueils bien connus comme le non-respect des délais ou le manque d'anticipation pour certaines étapes clé du projet.

Il faudra donc penser cette migration vers Lync 2013 en découpant et en intégrant chaque donnée et chaque action en 5 phases regroupant les 42 processus selon le PMP. Et parce qu'un projet est par définition temporaire, il y aura donc la première phase concernant le démarrage du projet, suivie du groupe de processus gérant la planification, puis l'exécution, pour finir par les processus de clôture. Tout au long de ces phases, nous utiliserons un cinquième groupe de processus concernant la surveillance et la maîtrise de la gestion du projet.

Enfin, il faudra s'attacher à définir pour chaque processus engagé les données d'entrée, les outils et techniques à utiliser et les données de sortie.

Voici donc une synthèse du Cycle de vie du projet Lync à travers les cinq groupes de processus : voir figure 1.

PHASE DE DÉMARRAGE

Dans le cadre d'un projet Lync, la phase de démarrage est évidemment importante car elle permet d'identifier les parties prenantes, avec une grille des rôles et responsabilités de chacun. On pourra ensuite informer au plus tôt les équipes techniques des prérequis et des impacts prévisibles sur l'environnement de production. D'autre part la tenue d'une réunion officielle lançant le projet de déploiement permet d'obtenir généralement la mobilisation des diverses personnes impliquées dans le projet. On devrait donc logiquement trouver les équipes suivantes :

- Réseau
- Téléphonie
- Poste de travail
- Sécurité

Contrairement au projet d'infrastructure classique (Exchange, Sharepoint, SQL Server), le déploiement de la solution Lync 2013 a une surface d'impact sur le système d'information plus importante, car elle nécessite d'une part la prise en compte de données « temps réels » encore peu présentes dans l'environnement informatique et dont la gestion n'est pas toujours familière aux équipes internes. D'autre part, ses besoins en communication et ses exigences réseaux doivent être rapidement assimilés par les parties concernées, ceci dans le but d'organiser les conditions environnementales permettant de déployer correctement la solution.

La phase de démarrage a donc dans le cas de Lync plusieurs objectifs. Elle va naturellement initier la phase de planification en fonction des prérequis matériels et logiciels, mais également préciser les exigences techniques, qui parfois peuvent s'avérer contraignantes à définir. Voir figure 2.

Figure 2

PHASE DE PLANIFICATION

La planification d'un projet Lync est marquée par quelques étapes clef qui pour certaines d'entre elles ont un impact global sur l'environnement de production. On trouve bien évidemment les opérations d'extension de schéma, la mise en place de passerelle de communication voix en coupure parfois du Pbx, ou la mise à disposition de certificats ou d'adresses IP publiques V4 qui sont parfois difficiles à obtenir. En outre, la disponibilité des équipes réseaux et des personnes ayant en charge la maintenance, en conditions opérationnelles, des équipements tels que les proxy inverses et les répartiteurs de charge est une contrainte de planification qu'il convient de ne pas négliger. N'oublions pas que Lync est un produit communiquant et va demander, plus particulièrement dans le cadre de scénarios basés sur une répartition de charge matérielle, la mise en place de paramétrages parfois évolués.

La phase de validation fonctionnelle (Vérification d'Aptitude) doit être ainsi particulièrement étendue car les fonctions Lync et les cas d'usage sont généralement nombreux. Ce sera notamment le cas si votre le projet comprend une phase de coexistence entre Office Communicator, Lync 2010 ou Lync 2013. Et si vous associez à cela les accès externes et la présence des fonctions mobiles sur Windows Phone, Iphone, Ipad, Android, vous aurez plusieurs cen-

taines de tests à faire pour valider l'ensemble des scénarios. Dans la plupart des cas, je vous rassure, les équipes techniques valident les fonctions clefs et migrent une population pilote importante et variée afin de vérifier que la plateforme est totalement opérationnelle.

Dans les entreprises de taille importante, tous les changements demandés, toutes les validations indispensables vont nécessiter l'établissement de demandes de changement qui elles aussi peuvent générer du délai. Toutes ses contraintes liées à l'organisation et à l'approvisionnement doivent impérativement rentrer en ligne de compte dans la planification du projet. Voir figure 3.

Figure 3

PHASE D'EXÉCUTION

La phase d'exécution du projet correspond aux étapes de déploiement de l'environnement Lync 2013 qui englobe les phases de conception puis d'installation des services de base (Services Frontaux, Monitoring, serveur SQL , serveur Edge, service Office Web App etc).

La phase de conception est, surtout dans l'environnement Lync, une étape majeure. Elle va permettre de définir précisément l'architecture souhaitée au vu des contraintes de disponibilité et des objectifs à atteindre. Et elle doit déboucher sur la livraison d'un document de spécifications techniques détaillées qui reprend l'intégralité des paramétrages, des choix de configuration, de publication, d'accès vers les futurs services Lync. Cette phase de conception doit aussi fournir aux équipes réseau des documentations indispensables telles que :

- La matrice des flux.
- L'estimation des consommations en bande passante.
- La définition des limitations de ces dernières (CAC).
- La priorisation des flux (Qos, si envisagé).

La documentation de spécifications techniques détaillées doit également préciser la liste complète des ports de communication, des Url utilisées, des noms de certificats et indiquer les contraintes de répartition de charges attendues (persistance de sessions, services répartis, etc.).

Cette documentation doit bien entendu faire l'objet d'une conception initiale et de mises à jour régulières, pour aboutir en fin de projet à un livrable reflétant parfaitement l'architecture déployée.

Les phases de déploiement répondent à une suite d'actions précises et interdépendantes qui sont pour la plupart correctement documentées sur le site de l'éditeur. Malgré cela, le déploiement des services Lync doit être réalisé par du personnel expérimenté maîtrisant la technologie associée.

Le déploiement de Lync, après une phase de conception correctement réalisée, ne pose pas de problème particulier, malgré son caractère relativement technique, comprenant le déploiement des services de bases, le paramétrage et la validation technique des services. Selon l'architecture envisagée et son niveau de complexité, l'installation de l'environnement de production va exiger plus ou moins de matériels complémentaires comme des répartiteurs de charge, des passerelles d'interconnexion voix, des téléphones IP, ainsi que la modification des services d'infrastructures (Dhcp, dns service proxy, Pare-feu). La maîtrise de ces équipements par les services internes ou prestataires associés permet ainsi de réduire fortement le temps d'installation et par conséquent les coûts du projet. L'approvisionnement en temps et en heure de ces matériels permettra de garantir le planning de livraison de l'infrastructure.

Même en cas de migration, les risques inhérents à cette étape sont faibles, car Lync 2013 s'installe à côté d'un environnement Lync 2010 ou OCS. Seules quelques étapes peuvent être considérées comme sensibles car ayant un impact sur la production. Parmi elles on notera :

- L'extension du schéma Active Directory.
- Le déplacement de la base de données CMS.
- Le basculement en production des services Edge.
- La bascule des interfaces PSTN vers les passerelles d'interconnexion dans le cadre d'une mise en coupure.

Coté processus de qualité, on s'attachera à vérifier plusieurs points techniques qui sont les suivants :

- Présence des derniers correctifs logiciels sur la partie serveurs mais également sur la partie cliente (Postes,

Téléphone IP).
• Absence de point de rupture unique sur les environnements à haute disponibilité.
• Vérification de problèmes de configuration avec les outils Best Practice Analyser.
• Documentation de l'installation.

SURVEILLANCE ET MAÎTRISE

Comme cité plus haut, l'installation d'une plateforme Lync fait appel à un savoir-faire plus ou moins conséquent selon le degré de complexité de l'environnement envisagé.

Si la plupart des sociétés désireuses d'utiliser Lync 2013 fait appel à des sociétés de services, la maîtrise du déploiement passe avant tout par une bonne compréhension des processus inhérents à la technologie. Nous conseillons par conséquent aux personnes désireuses de suivre, dans l'optique d'une meilleure maîtrise de l'exploitation future de ces environnements, les processus de déploiement, soit de recourir donc à une formation préalable, soit de s'auto-former. La documentation technique en français disponible sur le site Technet, les webcast des Techdays disponibles en ligne, ou les articles d'ITPro vous permettront sans souci d'acquérir un niveau de base nécessaire et suffisant. La maîtrise des fonctions de base et des processus généraux Lync 2013 optimisera par conséquent les opérations de transfert de compétence.

D'autre part, nous vous conseillons également de procéder au déploiement et aux recettes unitaires des fonctions déployées. La validation séquentielle par ordre d'importance des services Sql, puis Frontaux, puis Edge est un grand classique. A chaque déploiement doit ainsi correspondre une validation standard basée à chaque fois sur un serveur unique. Viendra ensuite la validation des services en commun (haute disponibilité), puis le passage en fonctionnement dégradé et la mesure de son impact côté client. Ces livraisons régulières de services permettront de recetter fonctionnellement étape par étape, le futur environnement de production. Compte tenu du nombre de fonctions disponibles, nous vous invitons fortement à procéder à la rédaction de fiches de tests unitaires pour être sûr de ne rien oublier.

Enfin, même si Lync 2013 n'est pas un gros consommateur de données, à l'instar de Microsoft Exchange, il va demander la mise en place d'un minimum d'opérations de sauvegarde et de restauration qu'il faudra maîtriser et documenter.

Comme dans la plupart des cas, l'ouverture du service devra se faire sur un panel représentatif d'utilisateurs avec lequel on prendra soin d'observer une période de validation à minima de 10 jours ouvrés. Là aussi, vous pouvez opter dans un premier temps pour l'ouverture du service uniquement depuis le réseau interne puis dans un second temps depuis l'internet. Cette ouverture en deux étapes vous permettra d'identifier plus facilement la source des problèmes techniques qui pourraient se poser et contribuera à l'amélioration de la maîtrise de vos processus.

PHASE DE CLÔTURE

La finalisation d'un projet Lync intervient généralement après une phase assez longue de Validation des Services Réguliers. Au cours de cette étape a lieu l'arrêt définitif des anciens services comme Office Communication Server ou des anciens systèmes de téléphonie, la maîtrise de l'exploitation des services par les équipes internes et l'ensemble des documentations remis et validé. L'absence de problèmes techniques courants va permettre d'arrêter les opérations de support et de mettre fin au projet. La phase de clôture permet également de faire le point avec les différents acteurs sur les aspects qualitatifs et organisationnels du travail effectué. C'est une étape importante qui permet d'apprendre et de pouvoir par la suite améliorer ou enrichir sa méthodologie. Et la rédaction du bilan projet devrait constituer le dernier des livrables.

Tout au long du déploiement de Lync 2013, grâce à la méthode PMP, vous aurez à cœur de formaliser les leçons apprises à chaque étape, à chaque processus, afin d'améliorer les compétences de chacun, quels que soient les projets à venir. Et en cela, la méthode PMP est particulièrement productive de progrès ! Vous aurez aussi remarqué l'intérêt de cette méthode pour atténuer de façon significative les soucis de délais, et donc de coûts, qui sont souvent à l'origine de nombreux échecs… Et même s'il on peut considérer que le PMP s'applique dans son entier aux projets de grande envergure, la trame qu'il apporte sera toujours très utile à tout chef de projet désireux de développer une efficience qualitative !

Alors, à vos projets, à vos déploiements, avec une nouvelle assurance grâce au PMP ! ■

Laurent Teruin
Architecte MVP Lync
http://unifiedit.wordpress.com/

Cécile Coste
Chef de Projet IT (indépendant)

Le travail n'est plus une question de lieu, mais bien de flexibilité

Quelle place pour le télétravail dans un environnement hyper connecté et mobile ?

› Par Arezki Hamadi

Marissa Mayer, PDG de Yahoo!, vient d'annoncer la fin du télétravail dans sa société à compter du mois de juin. Laissons la question des impacts de cette décision sur la productivité et l'attractivité de la société à ceux que cela intéresse pour nous concentrer sur le problème de fond : les répercussions de l'évolution des modes de travail sur l'IT des entreprises ces dernières années.

Les lieux de travail et postes de travail statiques sont dépassés, n'en déplaise à certains. Et les défis que doivent relever les administrateurs IT dépassent de loin le cadre du contrôle du télétravail. Il leur faut trouver des solutions économiques pour garder le contrôle de leur infrastructure informatique tout en embrassant les actuelles tendances de la mobilité, de la réglementation du Cloud Computing, de la sécurité et de la consumérisation de l'IT.

Trois critères définissent la solution idéale :

• La sécurité. Les ressources informatiques des entreprises sont désormais accessibles via pléthore d'applications et de terminaux, ce qui multiplie les risques sécuritaires. Les DSI doivent donc mettre en place des mesures de sécurité applicables à une multitude de logiciels et de plates-formes.

• L'automatisation. Habitués aux nouvelles technologies grand public, qui leur donnent instantanément accès aux services qu'ils demandent, les salariés se montrent plus exigeants vis-à-vis des technologies informatiques de leur entreprise. Automatiser les tâches IT standard permet justement d'alléger les sollicitations du service d'assistance IT.

• La flexibilité. Selon Forrester Research, 12 millions de personnes utilisent au moins 3 terminaux connectés et 7 applications par mois. Les services IT doivent investir dans des solutions évolutives pour garder le contrôle des données de l'entreprise tout en laissant les salariés libres d'y accéder depuis le terminal de leur choix, partout et à toute heure.


Arezki Hamadi

› Les lieux de travail et postes de travail statiques sont dépassés, n'en déplaise à certains.

Les employés veulent désormais pouvoir accéder immédiatement aux technologies dont ils ont besoin, 24h/24 et 7j/7. Tenter de les enchaîner à leur bureau n'y changera rien. Il est temps de se préparer à leur fournir les services à la demande qu'ils attendent tout en instaurant les règles de sécurité qui s'imposent et en posant les bases solides de l'architecture IT de demain. ■

Arezki Hamadi
Directeur de Comptes, RES Software France
RES Software

Pour aller plus loin sur ITPro.fr

Les salariés unanimes sur le télétravail
bit.ly/salaries-teletravail

La vidéoconférence chute en 2012
bit.ly/videoconference-chute

« Sur iTPro.fr, nos experts vous accompagnent au quotidien pour vous aider à tirer le meilleur profit de vos environnements IT ... »

En ligne sur iTPro.fr, 7 chaînes d'information et de formation des experts en technologies informatiques d'entreprise, par les éditeurs de IT Pro Magazine.

Une bibliothèque de ressources éditoriales exclusive pour vous accompagner dans la gestion et l'optimisation de vos environnements IT Professionnels.

- Chaînes thématiques
- + 2800 Dossiers IT
- Guides exclusifs
- 7 Flux RSS
- Newsletters hebdos
- Videos &Webcasts
- IT Virtualisation
- Windows Server
- IT Collaboration
- Exchange Server
- Power Systems
- SQL Server
- Club Abonnés
- Boîte à Outils
- Trucs & Astuces
- Hub éditoriaux
- Hors-Série
- Livres blancs...

Bénéficiez d'une richesse éditoriale incomparable ... connectez-vous !

Suivez-nous sur Twitter : www.twitter.com/itprofr

Partagez sur Facebook : www.facebook.com/www.itpro.fr

iTPro.fr

La bibliothèque éditoriale du site iTPro.fr est constituée de plus de 2800 dossiers technologiques signés par les meilleurs experts francophones et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT basés sur les principales technologies informatiques d'entreprise en termes d'infrastructure serveurs, réseaux, plate-forme de collaboration, mobilité d'entreprise et de virtualisation.

CONCEPTION & RÉALISATION : STUDIO IT MEDIA

Virtualisation : VMware ou Citrix ? … et pourquoi pas Hyper-V 3.0

› Par Olivier Mendes

Installer un système d'exploitation dans une ou plusieurs machines virtuelles et les faire fonctionner simultanément sur un seul serveur physique, est un concept qui est aujourd'hui familier. Mais la virtualisation ne s'arrête pas à la simple consolidation de serveurs physiques en serveurs virtuels (P2V). Pour les DSI qui souhaitent réduire leurs coûts d'infrastructure et renforcer la continuité métier, progresser vers la virtualisation des postes de travail et des applications est un chemin qu'il va falloir arpenter. Des projets de virtualisation sont déjà en cours de déploiement dans des entreprises qui se veulent innovantes et toujours précurseurs. Lorsque l'on décide de développer son offre de virtualisation d'infrastructure, l'intérêt n'est pas juste d'empiler les technologies et d'être au top, mais plutôt de construire le SI de demain, plus réactif, moins énergivore et où les tâches d'administration et de maintenance seront rapides et simples.

La virtualisation, loin d'être encore d'utilité publique, apporte déjà des avantages indéniables, comme par exemple :

- Allouer dynamiquement du temps processeur en fonction des besoins.
- Permettre la possibilité d'une erreur de dimensionnement des ressources serveur pour une application (le resizing étant transparent).

Pour aller plus loin sur ITPro.fr

Hyper-V 3.0 : Les améliorations de la plateforme
bit.ly/hyper-v-3-ameliorations

Hyper-V 3.0 taillé pour le cloud privé
bit.ly/hyper-v-cloud-prive


Olivier Mendes

» L'avancée technologique et l'investissement fournis par Microsoft dans le développement d'Hyper-V porte enfin ces fruits.

• Utiliser de façon optimale les ressources physiques en répartissant les machines virtuelles en fonction de leurs charges.
• Faciliter la livraison de nouveaux environnements de qualification, pré-production et production par le déploiement et la migration de machines virtuelles standardisées.
• Économiser sur le matériel, la consommation électrique, la maintenance, le support, la surface au sol…
• Isoler les différents utilisateurs d'une même VM.

Il est clair que tous ces avantages, et bien d'autres, sont accessibles au travers de la virtualisation. Avec l'évolution de l'offre proposée par les éditeurs de solution, la question qui se pose à présent n'est pas tant de savoir ce que la virtualisation peut fournir comme bénéfices, mais davantage de choisir « le bon produit », celui qui sera simple à déployer dans mon infrastructure et qui convient à mes besoins.

TABLEAU 1

	Microsoft	vmware	CITRIX
Version	Hyper-V 2012	vSphere 5.1	XenServer 6
Edition	Datacenter	Enterprise Plus	Platinum Edition
Host / Logical Processors	320	160	64
Host / Physical Memory	4TB	2TB	1TB
Host / Virtual CPUs per Host	2028	2028	75
Host / Max Cores per CPU	illimité	illimité	illimité
VM / Virtual CPUs per VM	64	64	16
VM / Memory per VM	1TB	1TB	128GB
VM / Active VMs per Host	1024	512	75
VM / Guest NUMA	Oui	Oui	Oui
Cluster / Maximum Nodes	64	32	16
Cluster / Maximum VMs	8000	4000	800
Storage / Supported Storage	SMB3 (new), virtual FC (new), SAS, SATA, iSCSI, FC	DAS, NFS, FC, iSCSI, SSD for Swap, FCoE (HW&SW), 16Gb FC HBA (NEW)	DAS, SAS, iSCSI, NAS, FC
Storage / Virtual Disk Format	.vhd - new (4KB sectors), vhd, pass-through (raw)	vmdk, raw disk (RDM)	vhd, raw disk (LUN)
Storage / Max Disk Size	64TB (vhd), 2TB (vhd), 256TB+ (raw)	2TB (vmdk), up to 64TB RDM (physical compatibility)	Limité
Storage / Thin Disk Provisioning	Yes (Dynamic Disks, Trim - new)	Yes (now with SE Sparse Disk - NEW)	Limité

Lors des derniers Techday's, de nombreux ateliers m'ont permis de découvrir des présentations d'Hyper-V sur Windows Server 2012 et cette solution enrichie, avec une version 3.0 plus avancée que jamais, pourrait bien être « enfin » l'outsider face au géant VMware et aux solutions Citrix. Il est nécessaire de mettre de côté les idées préconçues sur un produit qui n'était, selon moi, pas à la hauteur des attentes de beaucoup d'entreprises. Aujourd'hui, j'ai révisé mon jugement et je pense qu'avec un produit comme Hyper-V 3.0, nous allons faire face à une mise en concurrence des solutions éditeurs lors de concertations sur la création de nouveaux projets de déploiement. Une révolution qui se fera sur un comparatif des services de chaque solution éditeurs et non plus sur le choix évident du leader du marché. Ce choix final risque certainement d'être plus délicat et de se reporter sur l'offre de virtualisation proposée par Microsoft.

POURQUOI CHOISIR HYPER-V ET WINDOWS 2012 ?

Force est de constater la forte valeur ajoutée des produits VMware et Citrix, mais il est tout aussi utile de connaître l'état des lieux des solutions proposées et d'en discerner une réelle alternative telle que Hyper-V. Avec l'arrivée de Windows Server 2012, Microsoft se pose enfin en véritable Outsider et démontre que sa solution Hyper-V a changé et gagne en maturité. Selon une étude d'IDC, en 2011, Hyper-V a connu une hausse de 62 % et a investi 27 % du marché en 3 ans. Ce nouvel hyperviseur va bouleverser la donne sur le marché de la virtualisation et, adjoint à la suite System Center 2012 SP1, Microsoft va sérieusement rivaliser avec les autres solutions du marché.

Utilisé seul, Hyper-V virtualise habituellement les serveurs, ce qui crée un environnement virtualisé pour des systèmes d'exploitation et des applications. En y ajoutant VDI (Microsoft Virtual Desktop Infrastructure), Hyper-V permet la virtualisation des postes clients. En utilisant App-V, la mise à disposition d'applications virtualisées devient un jeu d'enfants.

3 types de virtualisation, un ensemble de technologies et de produits organisés autour d'une administration centralisée et une connectivité avec le Cloud sont mis à disposition par Microsoft pour une solution complète tournée vers les entreprises.

LES BÉNÉFICES D'HYPER-V 3 FACE À LA CONCURRENCE

L'avancée technologique et l'investissement fourni par Microsoft dans le développement d'Hyper-V porte enfin ces fruits. Avec de nouvelles fonctionnalités, telles que Hyper-V Replica, la taille des clusters passe à 64 nœuds et 8 000 machines virtuelles, le double de la solution VMware.

Un bon tableau vaut mieux que tous les mots. Voici donc le détail des principaux éléments qui caractérisent les trois offres de virtualisation les plus utilisées (voir tableau 1).

La comparaison est rapide, mais donner dans cet article la totalité des différences entre les solutions n'est pas vraiment adapté. Aussi, je vous invite à récupérer le détail des configurations présentées sur les liens indiqués en fin d'article.

L'offre de Microsoft vient de passer un cap et, avec Hyper-V 3.0, Windows Server 2012 et System Center 2012, l'intégration et la gestion de la virtualisation en entreprise sont grandement facilitées. De plus, le coût des licences relativement bas, est un avantage supplémentaire par rapport aux solutions VMware.

Pour ceux d'entre vous qui se souviennent de la guerre des navigateurs web, au milieu des années 90, Netscape était le leader du marché et Microsoft ramait derrière. Lorsque le géant endormi a subitement saisi l'importance stratégique des navigateurs et qu'il a investi toutes ses forces et moyens dans la bataille avec Internet Explorer, Microsoft a su s'imposer face à la concurrence.

Nous verrons bien comment VMware va réagir à cette entrée en matière et si les clients de VMware vont être attirés par le chant des sirènes Microsoft et changer de technologie… L'avenir nous le dira, mais pour Hyper-V, l'avenir commence cette année. ■

Sources :

- http://download.microsoft.com/download/E/8/E/E8ECBD78-F07A-4A6F-9401-AA1760ED6985/Competitive-Advantages-of-Windows-Server-Hyper-V-over-VMware-vSphere.pdf
- http://www.citrix.com/content/dam/citrix/en_us/documents/products/citrixxenserver6configurationlimits.pdf

Olivier Mendes
Expert technique Microsoft
Atos
Département Expertise & Conseil Technologique

Collaboration et communication vidéo

Découvrez la suite de vidéo-communication Aastra BluStar™

La solution Aastra BluStar™ marque une nouvelle ère dans les communications d'entreprise, renforçant la position d'Aastra comme un acteur mondial majeur sur le marché des communications unifiées.

Découvrez l'Aastra BluStar 8000i avec son écran tactile de 13 pouces et une qualité de diffusion audio et vidéo équivalente à une collaboration naturelle.

Adoptez l'Aastra BluStar for PC, une vidéo HD, un accès à l'ensemble de fonctions de Communications Unifiées et de Collaboration (UCC) à partir d'un client PC.

Téléchargez notre environnement sur vos tablettes et smartphones avec Aastra BluStar for iPhone et Aastra BluStar for iPad.

Visitez notre site : **www.blustar.aastra.fr**

Microsoft

OVH.COM

L'ENTREPRISE FAMILIALE DEVENUE HÉBERGEUR MONDIAL

OVH.COM OPTIMISE SON ACTIVITÉ GRÂCE À WINDOWS SERVER 2012.

OVH.com est le premier hébergeur européen de sites web. Avec ses 11 centres de données en Europe, cette entreprise française possède également au Canada la plus grande « ferme de serveurs » au monde. OVH.com héberge ainsi 150 000 serveurs actifs, 18 millions d'applications Web et gère 3 millions de noms de domaine. Séduit par les nouvelles fonctionnalités de Windows Server 2012, OVH.com souhaitait être parmi les premiers à proposer à ses clients un hébergement basé sur la toute dernière plateforme web de Microsoft.

En choisissant Windows Server 2012 et IIS 8.0 pour l'hébergement de sites dynamiques, OVH.com a pu augmenter de 25 % la densité de sites par serveur, tout en abaissant de 30 % la quantité de mémoire utilisée par site. Windows Server 2012 lui a ainsi permis d'accélérer la fourniture de services de plateforme web Microsoft et de réduire ses frais d'exploitation.

Découvrez l'aventure complète d'OVH.com et ce que Windows Server 2012 peut offrir à votre entreprise : microsoft.com/ws2012

Windows Server 2012

CLOUD PAR ESSENCE

microsoft.com/ws2012