Sécurité: IBM, avec ISS, pousse les services managés

Profitant de la publication d'un rapport semestriel sur les vulnérabilités, (*), IBM France a fait le point ce 1er octobre, avec la presse, sur son offre de services managés en matière de sécurité des SI.

Il s'agit d'une offre orchestrée par **IBM GTS** (Global Technology Services). Sur le terrain c'est la compétence des équipes issues, en grande partie, de l'acquisition d'ISS (Internet Security Systems) en 2006. Cette 'task force' est désignée ainsi: « ISS X-Force Research & Development team ».

Cette compétence se traduit par trois volets principaux: un volet « recherche », un autre sur la technologie et le 3è sur les solutions », ont expliqué Loic Guézo, responsable technique offre ISS chez IBM France, et Jean-Paul Ballerini, responsable technique ISS au sein d'IBM 'South West Europe » (basé à Bologne).

« *Nous avons développé un « cadre général de gouvernance' qui prend en comptes nos ressources d'expert (autour de l'offre Tivoli), nos solutions « data & information » (encryption, sécurité des données stockées), application & process (l'offre Rational, complétée par l'expertise Watchfire, récemment racheté), « network service & end-point », l'infrastructure physique et, enfin, cette nouvelle offre, celle de services managés*« .

En pratique, c'est l'expertise et les ressources d'ISS qui sont immergées dans **9 'SOC**' ou ***Security operation centers***'. Ces 9 centres sont répartis entre les Etats-Unis (4), l'Europe (2), l'Asie/Pacifique (2) et un tout nouveau à Bengalore (Inde) – ce qui permet à IBM GTS de proposer, en 24h sur 24, 7 jours sur 7, des services managés pour la supervision d'équipements de sécurité.

Ces centres d'opération ont comme mission de **superviser à distance les équipements de sécurité les plus critiques**, notamment les pare-feu (firewalls : 50% des accès web dans les entreprises ne seraient pas filtrés !) mais également, et les consultants d'IBM insistent, les **dispositifs de prévention d'intrusion** (***IPS***) qu'un certain nombre d'entreprises auraient tendance à sous-estimer. IBM les proposent au sein du datacenter (avec une efficacité, en débit, allant jusqu'à 40 Gbps) et/ou en périphérie.

Et de citer par exemple le cas des **attaques Conficker** qui ont secoué les responsables sécurité IT à partir de novembre 2008. Le dispositif mis en place par IBM ISS protégeait ses clients de l'exploitation de cette vulnérabilité avec deux ans d'anticipation.

Cette X-Force team d'IBM ISS intervient dès à présent auprès de **3.700 clients**'managés' en sécurité, ce qui représente, au total, 26.000 équipements sous contrat, totalisant 6 millions d'événements 'sécurité' suivis quotidiennement dans 133 pays. IBM recense 250 incidents 'sécurité' par jour, soit une attaque par semaine, par client!

Cette équipe X-Force, avec ses développeurs, compte environ 200 personnes, récemment regroupées à Atlanta.

L'exécution de ces services managés de sécurité est accessible **via un portail web** de pilotage

d'infrastructure, installé chez le client: il s'agit notamment du monitoring à distance des équipements de sécurité critiques, donnant lieu à l'affichage d'alertes, l'édition d'indicateurs, des tableaux de bord et des rapports de synthèse.

La négociation du contrat de service avec le client commence par une mise à plat des règles de sécurité appliquées. « *Nous définissons avec lui, très précisément, ses règles et objectifs de 'sécurité'*.

Le service peut aller jusqu'à la mise en quarantaine de serveurs et/ou de postes de travail, dans un délai de quelques minutes, avec avertissement envoyé au client, donc avec son aval ».

Le prix de ces services managés est établi à partir de multiples paramètres comme le nombre des changements des règles, le nombre d'équipements supervisés, les délais d'intervention, etc. Il s'agit d'une prestation avec un coût fixe mensuel, sans investissement préalable.

Trois niveaux de service sont proposés: « standard », « select » ou « premium ».

En France, comme ailleurs, ces services managés « sécurité » sont déjà proposés à travers des partenaires, intégrateurs ou prestataires de services d'infogérance, utilisant cette infrastructure d'IBM en « marque blanche ».

Les profils de clients?

« *Ces sont des entreprises qui reconnaissent qu'elles n'ont pas les compétences ni les ressources suffisantes pour gérer 24h/24 leur infrastructure réseau; ce sont des contrats de* 'tasking'*, avec clause de réversibilité. Les personnes qui suivent quotidiennement la sécurité -et l'application du contrat – peuvent, dés lors dédier plus de temps à la prévention, à la planification en amont, etc*. »

Ce ne sont pas que des grands comptes. IBM cite le cas d'un sous-traitant dans le domaine de l'aéronautique et de la défense, qui doit disposer d'un service 24h24 sur ses sites en Europe, pour répondre aux exigences de son client, un EADS, par exemple. Ou encore le cas d'un entreprise moyenne qui ouvre des implantations dans des pays émergents, comme la Turquie, en se gardant la souplesse de pouvoir réduire la voilure à tout moment.

Le prix généralement constaté est de l'ordre de 1.000 euros par mois, par équipement supervisé.

IBM va jusqu'à proposer une forme de pari: diminuer de 50% les coûts d'exploitation de cette maintenance des équipements sécurité ; car IBM constate qu'en moyenne chaque poste d'astreinte d'un service 24h/24 7Jours/7 nécessite la rotation de 6 personnes!

Les informations et la communication utilisent plusieurs formes, selon les souhaits du client: emails, SMS… IBM propose également des 'chats' en direct autour des incidents majeurs, des 'wickis', ainsi que la constitution de bases de connaissances, au delà des bulletins d'alerte.

___

(*) Publication d'un rapport statistiques détaillé, à mi-2009: « ***IBM ISS X-Force 2009 mid-year trend and risk report***',

C'est un rapport d'une centaine de pages, riche, détaillant les vulnérabilités , recensant les principaux malwares, leur impact, leur niveau de dangerosité ou « sévérité », y compris les attaques

par injections automatiques dans des requêtes SQL, ou encore les failles des navigateurs Internet, etc. Source: IBM ISS X-Force (Internet Security Systems) Research & Development team

au sein de IBM Global Technology Services

AGENDA : 'Virtualization Tour 2009'*Venez participer dans votre région au grand rendez-vous sur la virtualisation organisé en partenariat avec IBM. Pour vous inscrire, consultez l'agenda, les dates et lieux de ce rendez-vous de la virtualisation* : cliquez ici ***LIVRE BLANC: Virtualisation du stockage IBM***
Présentations générales, techniques ou détaillées. Laissez-vous guider dans la virtualisation du stockage IBM: cliquez ici