A quel prix sécuriser les services Web?

Amsterdam.- Pas de doute: les 'Web services' prennent de l'importance dans la stratégie de productivité des entreprises. Élément d'intégration des applications, que permettent-ils en pratique? De consulter plusieurs applications et de les faire coopérer via des passerelles dynamiques; et cela sans avoir à développer des outils d'intégration protéiformes qui coûteraient à chaque fois une petite fortune… D'où leur impact en réduction des coûts. Pourtant, force est d'admettre qu'il faut ajouter le prix de la protection ou sécurisation. Phillip Hallam-Baker, architecte sécurité chez Verisign ne le nie pas: «*Ces services doivent être fiables et sécurisés, d'autant plus qu'ils sont fondés sur un échange libre et dynamique de données et de services*». Et d'énumérer 5 facteurs clés (cf. encadré ci-après). **Des protocoles bientôt normalisés?** Ces différents points sont aujourd'hui traités, avec force standards ou normes. Ainsi, Verisign, Microsoft et IBM ont récemment collaboré, par exemple, pour instaurer la spécification *Web service Security* (WS security): elle vise à ajouter une couche de protocoles de sécurité. Sur cette base, ont été conçues des spécifications complémentaires dont notamment WS-Policy (pour déterminer les procédures à appliquer), WS-Trust (pour créer un espace de confiance), etc. Un constat découle de cette approche: c'est toute l'infrastructure des échanges qui doit être sécurisée. Il faut savoir à qui faire confiance puisqu'il s'agit de données stratégiques. Le paiement électronique en ligne, sur Internet, fait également partie des engagements. Or, on ne peut pas installer de tels services en y «plâtrant» toute une série d'utilitaires de sécurité. Une base commune ou infrastructure dynamique s'impose au préalable: les services évoluent, de même que les menaces. En clair, il est indispensable de penser la sécurité des Web services en termes d'intégration à leur architecture. C'est l'un des thèmes majeurs abordés à la Conférence RSA d'Amsterdam cette année. Un nombre croissant d'acteurs coopèrent pour permettre aux développeurs de créer des Web services sûrs et fiables ou plus exactement de fournir des services de sécurité via une seule et même interface programmable (API) unificatrice. Mais on est encore loin du compte: il n'existe pas vraiment de standard en la matière. **Des maux mais pas de chiffres…** Comme d'habitude, pas de chiffres à l'occasion de cette conférence néerlandaise de RSA Security qui, pourtant, réunit une belle brochette d'experts. On y répète que le retour sur investissement en matière de sécurité informatique ne se calcule pas… sauf s'il s'agit de gestion des identités et des accès (le domaine de prédilection de RSA, comme il se doit…). C'est après coup (« post mortem » dit le cabinet Media Group) que cela se mesure parfois: par exemple, le compte-rendu fait par les utilisateurs, lorsque l'on s'aperçoit qu'à quelque chose «malheur» est bon, ou plus exactement, qu'un système de sécurité apporte des avantages imprévus (sic). Il reste que le malheureux responsable sécurité, toujours en quête d'argent pour appliquer la politique édictée par la direction, a toujours du mal à obtenir un budget. Et lister tous les malheurs qui attendent l'entreprise n'émeut guère. Selon le cabinet Quocirca, seules les organisations publiques semblent y être sensibles. Ainsi, la British Chamber of Commerce, signale que «*93 % des entreprises ont connu l'an passé au moins une tentative d'intrusion et une attaque virale. Que 61 % d'entre elles ont subi un crime informatique et que 70 % de celles qui ont essuyé un désastre sur leurs données vitales ne seront plus là pour en parler l'année prochaine*». **Cent fois remettez votre ouvrage…** Dans ce contexte, RSA Microsoft et Accenture ont décidé de coopérer très activement. RSA ClearTrust est désormais intégré au coeur de la technologie de gestion des identités et des accès de Microsoft. Idem pour les Web services. Microsoft intégrera le code source de RSA SecurID dans son serveur ISA (*Internet Security & Acceleration Server*). Même principe avec Accenture: une alliance dans le cadre de ses

solutions Accelerated Identity & Access Management. Ils sont trois à coopérer: Accenture, RSA (via l'offre ClearTrust) et Thor (via son progiciel Xellerate). Cette dernière, une jeune société, connaît un succès croissant sur le marché de la sécurité. Objectif de cette alliance: fournir une solution globale d'infrastructure de sécurité allant des services d'authentification aux ressources de sécurisation en passant par le contrôle d'accès, la signature unique (ou SSO, *Single Sign On*) et l'administration des utilisateurs -l'un des rares points où se mesure le retour sur investissement. **Cinq facteurs clés à considérer**

Selon Phillip Hallam-Baker, architecte sécurité chez Verisign, il faut prendre en compte **cinq facteurs clés**: – une très haute disponibilité: car ces services doivent être faciles d'accès aussi bien via des répertoires publics (moteurs de recherche inclus) que privés (dans le référentiel de l'entreprise); – une confidentialité absolue: les communications doivent être protégées contre toute indiscrétion ; – une totale intégrité des données: pas d'altération durant leur transmission ; – l'authentification du service pour toute personne s'y connectant ; – la mise en place de procédures d'autorisation garantissant que l'accès reste limité au service défini, en prenant en compte les données sensibles.