

Pour Juniper Networks la sécurité du réseau de l'entreprise passe par la protection des smartphones

Juniper Networks élargit la déclinaison de son offre de gestion du réseau de l'entreprise à la sécurisation de sa périphérie, à savoir les terminaux mobiles. « *Il est Important de continuer à décliner cette stratégie au terminal pour sécuriser l'ensemble du réseau* », explique **Bruno Durand**, responsable France et Europe du Sud de Juniper. Car l'usage des smartphones, notamment, s'est tellement généralisé qu'il devient difficile pour l'entreprise de contrôler les accès de son systèmes d'information.

« *En France, 70 % des utilisateurs interrogés accèdent au réseau de l'entreprise avec un terminal, que ce soit pour consulter sa messagerie ou pour accéder aux applications* », rappelle le dirigeant en s'appuyant sur les résultats d'une étude menée en octobre 2010 par KRC Research et Synovate pour le compte de Juniper auprès de 7000 personnes sur 7 pays. En France toujours, 68 % des sondés le font à l'insu de leur hiérarchie (81 % globalement). Et 19 % ne protègent pas leur smartphone d'un mot de passe (25 % aux Etats-Unis). On imagine les risques que font porter les utilisateurs pour l'entreprise en cas de perte ou vol du terminal, sans parler des *malwares*.

Les applications malveillantes sont en effet de plus en plus actives dans le monde de la mobilité. « *Sur les quinze plus grandes entreprises américaines, 5 % des appareils mobiles sont infectés par des malwares, soutient Bruno Durand qui ajoute que une application [légitime] sur vingt peut avoir l'autorisation de passer des appels sans avertir l'utilisateur* ». Plus inquiétant, 61 % des virus sur smartphones sont capables d'espionner les communications à l'insu de l'utilisateur, même hors communication. Et 17 % s'apparentent à des chevaux de Troie transmis par des textos qui aboutissent à la possibilité d'effectuer des prélèvements sur le compte bancaire de l'utilisateur (pour celui qui accède à ses données financières depuis son téléphone mobile). « *Ça paraît de la fiction mais c'est la réalité aujourd'hui* », affirme le dirigeant.

La totalité des OS mobile supportée

Face à ces risques d'intrusion et d'usurpation d'identité, « *l'entreprise peut limiter les accès en fonction des utilisateurs mais c'est très compliqué de voir le terminal mobile et sa version de l'OS. Soit elle interdit tout mais réduit la productivité de ses employés, ce qui est difficilement concevable aujourd'hui, soit elle autorise les accès mais de manière sécurisée. C'est ce que nous proposons aujourd'hui.* »

L'offre Junos Pulse Mobile Security se compose d'un ensemble d'applications (antivirus, pare-feu personnel, antimalware/antispam) et de services (protection contre la perte et le vol d'information, administration et contrôle des services), avec notamment la possibilité, en cas de perte ou vol, de géolocaliser le terminal, de le bloquer et même d'effacer les données qu'il contient (après les avoir sauvegardées en ligne, bien entendu). Le tout à distance par l'administrateur ou depuis un portail mis à la disposition de l'utilisateur.

La suite de sécurité s'intègre désormais comme un élément de la plate-forme globale Junos Pulse

de Juniper. Elle permet aux entreprises de sécuriser l'accès à ses applications et à la messagerie depuis les terminaux mobiles tout en protégeant les données et le réseau. La solution s'appuie notamment sur l'offre VPN SSL de Juniper, qui établit un tunnel sécurisé entre le réseau de l'entreprise et le terminal, et déjà déployée par quelques dizaines de milliers d'entreprises dans le monde. L'offre présente également l'avantage de supporter la quasi totalité des plates-formes mobiles, de l'iPhone à Android en passant par Symbian, BlackBerry et Windows Mobile. Autant dire que les tablettes seront (sont déjà) prises en compte. Ce qui prépare l'avenir puisque Forrester Research estime que le nombre de smartphones et tablettes sera supérieur à celui des ordinateurs portables dès 2012.

Des grands comptes aux opérateurs

Du coup, Juniper vise aussi les opérateurs qui pourront proposer la sécurisation des terminaux mobiles à leurs clients, soit comme option à l'offre de base, soit comme produit d'appel pour se distinguer de la concurrence. L'offre pousse même le service jusqu'à pouvoir proposer un mode de contrôle parental qui permettra (selon la législation en vigueur dans le pays) de surveiller l'usage que font les enfants et adolescents de leurs smartphones, de leur géolocalisation physique aux photos qu'ils téléchargent.

L'opérateur britannique BT est déjà client. Tout comme IBM. *« Nous sommes en discussions avancées avec l'intégralité des acteurs opérateur du marché et les entreprises qui ont compris que la porte d'entrée du réseau est le terminal mobile désormais »*, illustre Bruno Durand. Une offre visiblement très attendue, donc. Elle est proposée à partir de 67 dollars par an par utilisateur. Si elle vise en priorité les grands comptes (par l'usage du réseau mis en oeuvre en mobilité), l'offre se veut très modulable avec des packs de 50 licences ou moins. Il n'en reste pas moins que l'entreprise doit prévoir un nouveau budget de fonctionnement. *« Certes, c'est un budget, nuance Bruno Durand, mais par rapport aux risques de pertes pour l'entreprise ou les particuliers, il faut le voir comme une assurance. Ce n'est pas une charge très élevée pour une entreprise. »*

Bien qu'encore difficile à chiffrer, le marché de la sécurité mobile est en plein essor. Si les éditeurs de solutions de sécurité comme Kaspersky ou McAfee commencent à élaborer des offres en ce sens, l'arrivée de Juniper Networks sur ce terrain démontre qu'il y a désormais un vrai besoin en la matière.