Internet : MobilitÃ© et sÃ©curitÃ© : un challenge stratÃ©gique pour les entreprises
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/12/2010 13:00:00

Force est de constater que la mobilitÃ© est dÃ©sormais une rÃ©alitÃ© concrÃ¨te pour les entreprises.

Structures multi-sites, collaborateurs nomades, banalisation des PC portables et autres pÃ©riphÃ©riques amovibles sont autant de facteurs qui ont permis Ã la mobilitÃ© de sâimposer comme incontournable dans un contexte professionnel. GÃ©nÃ©ratrice de gain de productivitÃ©, cette derniÃ¨re doit nÃ©anmoins Ãªtre encadrÃ©e afin de se prÃ©munir de tout dÃ©sagrÃ©ment.

Les aspects liÃ©s Ã la sÃ©curitÃ© sont donc un prÃ©-requis incontournable Ã prendre en compte. Rappelons-nous des rÃ©cents exemples ayant eu des consÃ©quences malheureuses pour des entreprises de renomâ¦ De maniÃ¨re gÃ©nÃ©rale, les postes nomades sont exposÃ©s Ã des environnements non contrÃ´lÃ©s et non sÃ©curisÃ©s ! Ils constituent donc une menace pour l'ensemble du rÃ©seau interne.

ConcrÃ¨tement, voici plusieurs cas de figure quâil convient de prendre en compte lorsque lâon se prÃ©occupe de la sÃ©curitÃ© en situation de mobilitÃ© :

- Un ordinateur portable volÃ©, perdu ou mal utilisÃ© menace lâintÃ©gralitÃ© des donnÃ©es critiques de lâentreprise.

- Les media de communications sans fil â clÃ©s 3G, points dâaccÃ¨s WIFI etc. â sont des cibles Ã©videntes que les pirates corrompent facilement, sâouvrant par lÃ mÃªme lâaccÃ¨s aux informations les plus sensibles de lâutilisateur

-Les ordinateurs portables mal utilisÃ©s sont des portes ouvertes Ã lâaccÃ¨s intrusif au rÃ©seau interne de lâentreprise.

Ces quelques exemples trÃ¨s concrets illustrent Ã eux seuls les dangers auxquels sâexposent les collaborateurs nomades qui manipulent des informations sensibles (fichiers clients, numÃ©ros de tÃ©lÃ©phone, fichiers comptables). Ces derniers doivent donc impÃ©rativement sâassurer de bÃ©nÃ©ficier dâune protection efficace. Nâoublions pas que la sÃ©curitÃ© doit Ãªtre prÃ©sente Ã tous les niveaux, y compris Ã lâintÃ©rieur des murs de lâentreprise.

Les postes nomades sont donc au centre de toutes les attentions. Ces derniers doivent pouvoir prendre en compte un certain nombre de paramÃ¨tres : gestion par liste blanche des points dâ□□accÃ¨s WiFi, routage obligatoire vers le VPN de lâ□□entreprise pour Ã©changer des donnÃ©es, contrÃ´le et autorisation des pÃ©riphÃ©riques externes, outil de dÃ©tection et de protections contre des attaques hÃ©tÃ©rogÃ¨nes, impossibilitÃ© dâ□□accÃ¨s aux donnÃ©es en cas de perte ou de vol de lâ□□ordinateurâ□¦

Le poste de travail nomade doit donc Ãªtre surveillÃ© en continu afin de ne pas Ãªtre Ã lâ□□origine dâ□□intrusions, de piratageâ□¦ Conscientes de ces risques, les entreprises et les administrations commencent Ã sâ□□Ã©quiper dâ□□outils dÃ©diÃ©s Ã la protection de leurs flottes de PC portables. Analyse comportementale et protection Ã base de signature, contrÃ´le des applications, technologies de chiffrement de donnÃ©esâ□¦ sont autant de dispositifs concrets et complÃ©mentaires qui se gÃ©nÃ©ralisent. Le travail de fond rÃ©alisÃ© par lâ□□ensemble des fournisseurs du marchÃ© a Ã©galement permis de rationaliser lâ□□approche liÃ©e Ã la sÃ©curitÃ© des pÃ©riphÃ©riques mobiles : approche unifiÃ©e et intÃ©grÃ©e, facilitÃ© de mise en Å□uvre etc. SÃ©curiser son parc nomade est donc dÃ©sormais une opÃ©ration possible et simple Ã mettre en Å□uvre.

Ces principaux Ã©lÃ©ments expliquent en grande partie lâ□□intÃ©rÃªt massif des entreprises et des organismes publics pour les sujets liÃ©s Ã la sÃ©curitÃ© des Ã©quipements portables. A n'en pas douter, nous devrions Ã court terme voir ce sujet se banaliser et sâ□□imposer comme un prÃ©-requis dans les politiques de sÃ©curitÃ© dÃ©finies par les RSSI et les Directions des SystÃ¨mes dâ□□Information.

Â

[**JÃ©rÃ´me Robert**, Responsable Marketing Produit de SkyRecon]